PCT/JP 2005/001437 PCT

26. 1. 2005

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

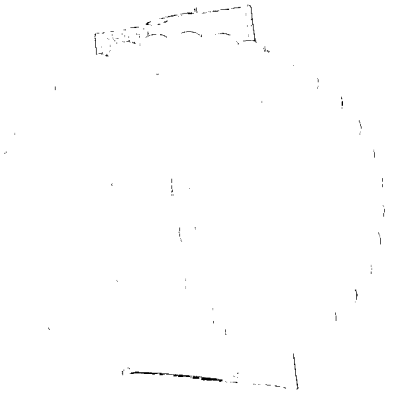
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００４年 １月２６日

出 願 番 号
Application Number: 特願２００４－０１６８８１

[ST. 10/C]: [ＪＰ２００４－０１６８８１]

出 願 人
Applicant(s): 日本電気株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年 ８月３０日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋

出証番号 出証特２００４－３０７７５７０

【書類名】　特許願
【整理番号】　35001256
【提出日】　平成16年 1月26日
【あて先】　特許庁長官　　殿
【国際特許分類】　G06F　1/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　古川　潤
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　寺西　勇
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100123788
　【弁理士】
　【氏名又は名称】　宮崎　昭夫
　【電話番号】　03-3585-1882
【選任した代理人】
　【識別番号】　100088328
　【弁理士】
　【氏名又は名称】　金田　暢之
【選任した代理人】
　【識別番号】　100106297
　【弁理士】
　【氏名又は名称】　伊藤　克博
【選任した代理人】
　【識別番号】　100106138
　【弁理士】
　【氏名又は名称】　石橋　政幸
【手数料の表示】
　【予納台帳番号】　201087
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0304683

【書類名】特許請求の範囲
【請求項１】
複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、
入力処理と、
出力処理とからなり、
前記入力処理では、前記複数の計算装置に、回路と、前記回路への入力ビットとが入力され、
まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする計算方法。
【請求項２】
複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、
入力処理と、
ElGamal暗号文準備処理と、
逐次置換再暗号処理と、
結果出力処理とからなり、
前記入力処理は、
前記複数の計算装置に複数のゲートから構成された回路の情報及び前記複数の計算装置に関する情報が入力される、情報入力ステップと、
関数の入力データを複数に計算装置の個数に分散したデータである複数の部分データを、それぞれの計算装置にそれぞれ一つずつ入力する分散入力ステップと、
からなり、
前記ElGamal暗号文準備処理は、
少なくとも一つの計算装置が、与えられた関数を実現する回路のゲートに対応したElGamal暗号文の集合を生成するElGamal暗号文準備ステップとからなり、
前記逐次置換再暗号処理は、
置換再暗号処理を各計算装置が順番に行う処理で、前記置換再暗号処理は、順番が回ってきた計算装置が、一つ前の順番に対応する計算装置からElGamal暗号文の集合を受け取る暗号文取得ステップと、
前記暗号文取得ステップにて受け取った暗号文の集合を順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化ステップと、
前記暗号文の置換と再暗号化ステップで生成したデータを、少なくとも次の順番の計算装置に公開するステップと、
からなり、
前記結果出力処理は、
前記逐次置換再暗号処理で生成された暗号文の一部を復号あるいは部分復号する部分復号ステップと、
前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文を復号する復号ステップと、
前記復号ステップで復号されたデータと、前記部分復号ステップで部分復号されたデータを用いて、回路の出力を評価する回路の評価ステップと、
からなることを特徴とする計算方法。
【請求項３】
複数の計算装置と、
複数の計算装置と通信する手段と、
入力処理手段と、
ElGamal暗号文準備手段と、

置換再暗号処理手段と、
結果出力処理手段と、
からなる関数を評価する計算システムであって、
前記入力処理手段は、出力を求めたい回路の情報と、前記複数の計算装置に関する情報と、前記複数の計算装置がそれぞれ前記回路の入力のどの部分を所持しているかという情報と、を入力し、
前記ElGamal暗号文準備処理手段は、与えられた関数を実現する回路のゲートに対応したElGamal暗号文の集合を生成するElGamal暗号文を準備し、
前記置換再暗号処理手段は、
順番が回ってきた計算装置が、一つ前の順番に対応する計算装置からElGamal暗号文の集合を受け取る暗号文取得手段と、
前記暗号文取得手段により受け取られた暗号文の集合の順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化手段と、
前記暗号文の置換と再暗号化手段を用いて生成したデータを、少なくとも次の順番の計算装置に公開する手段と、
からなり、
前記結果出力手段は、
置換再暗号処理手段で生成された暗号文の一部を復号あるいは部分復号する部分復号手段と、
前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文の自分に関する暗号化を復号する復号手段と、
前記複数の計算機が前記復号手段で復号したデータと前記複数の計算機が前記部分復号手段で部分復号されたデータを用いて回路の出力を評価する回路の評価手段と、
からなることを特徴とする計算システム。
【請求項４】
請求項２に記載された計算方法において、
前記各ゲートに対応するElGamal暗号文の集合は、前記各計算装置が各ゲートに対応して生成した秘密鍵のElGamal暗号文の集合であり、
前記ElGamal暗号文を生成するのに用いた公開鍵は、このゲートに入力される二つの信号を生成するゲートに対応する公開鍵の和であることを特徴とする計算方法。
【請求項５】
前記請求項２に記載された計算方法において、
前記入力処理として、各計算装置にElGamal暗号方式の領域変数を入力するステップが行なわれ、
前記ElGamal暗号文準備処理として、各前記計算装置が、各前記回路の各ゲートに対応して、ElGamal暗号文の秘密鍵を生成するゲート秘密鍵生成ステップが行なわれ、
各計算装置では、
前記ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応するゲート公開鍵を生成するゲート公開鍵の生成ステップと、
前記ゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成するゲート公開鍵の正当性の証明生成ステップと、
前記ゲート公開鍵の正当性の証明生成ステップにて生成したゲート公開鍵の正当性の証明を公開するゲート公開鍵の正当性の証明公開ステップと、
各前記回路のゲートで回路への入力が直接入力されるゲートに対応して、ElGamal暗号文の秘密鍵を生成する入力のゲート秘密鍵の生成ステップと、
前記入力ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応する入力ゲート公開鍵を生成する入力のゲート公開鍵の生成ステップと、
前記入力のゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成する入力のゲート公開鍵の正当性の証明生成ステップと、
前記入力のゲート公開鍵の正当性の証明生成ステップにて生成し入力の公開鍵の正当性

の証明を公開する入力のゲート公開鍵の正当性の証明公開ステップと、
その他の各計算装置が生成して公開したゲート公開鍵を取得するゲート公開鍵取得ステップと、
前記ゲート公開鍵取得ステップにおいて取得したゲート公開鍵を統合するゲート公開鍵の統合ステップと、
前記ゲート公開鍵の統合ステップにおいて統合したゲート公開鍵により、この計算装置が生成したゲート秘密鍵を暗号化するゲート秘密鍵の暗号化ステップと、
前記ゲート秘密鍵の暗号化ステップにおいて生成したゲート秘密鍵の暗号文を公開するゲート秘密鍵の暗号文の公開ステップと、
前記ゲート秘密鍵の暗号文の正当性証明を生成するゲート秘密鍵の暗号文の正当性の証明生成ステップと、
前記ゲート秘密鍵の暗号文の正当性の証明生成ステップにおいて生成したゲート秘密鍵の暗号文の正当性の証明を公開するゲート秘密鍵の暗号文の正当性の証明公開ステップと、
各計算装置に入力された回路の入力の部分に対応する暗号文を生成する入力の暗号文生成ステップと、
前記入力の暗号文生成ステップにて生成した回路の入力の部分に対応する暗号文の正当性の証明を生成する入力の暗号文の正当性の証明生成ステップと、
前記入力の暗号文の正当性の証明生成ステップにおいて生成した証明を公開する入力の暗号文の正当性の証明公開ステップと、
出力のゲートに対応する暗号文を生成して公開する出力の暗号文の生成ステップと、
を含み、
前記置換再暗号処理が、
前記ゲート秘密鍵の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化するゲート秘密鍵の暗号文の置換と再暗号化ステップと、
前記入力の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化する入力の暗号文の置換と再暗号化ステップと、
前記出力の暗号文の集合の順番をあらかじめ決められた許された置換方法から無作為に一つの置換を選んで入れ替えて再暗号化する出力の暗号文の置換と再暗号化ステップと、
前記ゲート秘密鍵の暗号文の置換と再暗号化ステップと入力の暗号文の置換と再暗号化ステップと出力の暗号文の置換と再暗号化ステップとにおいてなされた置換と再暗号化の正当性の証明を生成し公開するゲート秘密鍵の暗号文と入力の暗号文と出力の暗号文の置換と再暗号化の正当性の証明生成と公開ステップと、
を含み、
前記結果出力処理の部分復号ステップが、
前記計算装置が互いに通信及び計算することで前記ゲート秘密鍵の暗号文を部分復号するゲート秘密鍵の部分復号ステップと、
前記計算装置が互いに通信及び計算することで前記入力の暗号文を部分復号する入力の暗号文の部分復号ステップと、
前記計算装置が互いに通信及び計算することで前記出力の暗号文を部分復号する出力の暗号文の部分復号ステップと、
前記ゲート秘密鍵の部分復号ステップと入力の暗号文の部分復号ステップと出力の暗号文の部分復号ステップとでなされた部分復号の正当性の証明を生成し公開するゲート秘密鍵と入力の暗号文と出力の暗号文の部分復号ステップの正当性の証明生成と公開ステップと、
を含み、
他の計算装置の公開した種々の正当性の証明を検証するステップを含む、
ことを特徴とする計算方法。

【請求項６】
複数の計算装置、入力手段、出力手段を含み、まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す計算システムであって、
前記入力手段では前記計算装置に回路の情報と、前記回路への入力ビットの一部とが入力され、
第ゼロ周目の計算は第一の計算装置が第一周目の計算を行う前に行い、
前記複数の計算装置には、
前記各周の計算に使用される送られてきたデータを取得するデータ取得手段と、正当性証明検証手段と、署名文検証手段と、第一の計算装置のみが行う第一計算装置特別計算手段と、乱数生成を行う乱数生成手段と、本計算を行う本計算計算手段と、本計算で行った計算の正当性を証明する正当性証明作成手段と、署名手段とデータ送信手段とからなり、
前記送られてきたデータは、別の計算装置から送られてきたデータと、データ本体と、データ本体に対する正当性証明と、署名文とからなり、
前記署名文は、前記別の計算装置から送られてきたデータと、前記データ本体と、前記データ本体に対する正当性証明との組に対する署名文であるようなデータで、
前記正当性証明検証手段は前記送られてきたデータ中の正当性証明を検証し、
前記署名検証手段は、前記送られてきたデータ中署名文を検証し、
前記本計算は前記乱数生成手段で生成された乱数を用いて計算し、
前記署名手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明との組に対する署名文を作成し、
前記データ送信手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明と前記署名手段で作成された署名文との組を送信する事を特徴とする計算システム。
【請求項７】
請求項６に記載された計算システムにおいて、
前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第一周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組である計算システム。
【請求項８】
請求項７に記載された計算システムにおいて、
各周の計算が、第一周目の計算手段と、第一周目以降の周の計算手段とからなり、
前記計算手段は、第ゼロ周目の計算手段では真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組を作成し、前記第一周目の計算手段が再暗号に使用する為の公開鍵を作成する再暗号用公開鍵作成手段と、送られてきたデータを変換するデータ変換手段と、秘密鍵変換手段と、乱数変換手段とからなり、
前記データ変換手段が、前記データ本体である暗号文の組を、真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる別の組に変換する為の手段であり、
前記秘密鍵変換手段が、前記データ変換手段の計算結果である暗号文達の組に使用されている秘密鍵を再暗号用公開鍵作成手段で作成された公開鍵に対応する秘密鍵に変換する手段であり、
前記秘密鍵変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、

前記乱数変換手段が前記データ変換手段の計算結果である暗号文達の組に使用されている乱数を変換する手段であり、
前記乱数変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組である事を特徴とする計算システム。
【請求項９】
請求項８に記載されている計算システムにおいて、
第一周目以降の周の計算手段が、第二周目の計算手段と第二周目以降の計算手段とからなり、
前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第二周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、
前記第二周目の計算手段が、
前記送られてきたデータの前記データ本体を変換してエルガマル暗号文もしくは楕円曲線エルガマル暗号文を作成する暗号変換手段と、前記送られてきたデータのデータ本体の暗号文達を部分復号する部分復号手段とからなる計算システム。
【請求項１０】
請求項９に記載されている計算システムにおいて、
第二周目以降の計算手段が、第三周目の計算手段のみからなり、第三周目の計算手段の前記本計算手段が、前記送られてきたデータをそのまま出力し、
前記正当性証明作成手段が空列を出力する計算システム。

【書類名】明細書
【発明の名称】多数の入力から関数を計算する方法および装置。
【技術分野】
【０００１】
本発明は、与えられた関数の入力が複数の装置に分散されて保持されている時に、これら装置が連動してこの関数の出力を計算する方法に関し、特に各装置が他の装置と行う通信回数が与えられた関数に依らず定数回で計算できる方法およびシステムに関する。
【背景技術】
【０００２】
与えられた関数の入力が複数の装置に分散されて保持されている時に、これら装置が連動してこの関数の出力を計算する方法方法の従来の技術として、 Beaver、Micali、Rogawayが文献「D. Beaver、S. Micali、and P. Rogaway、『The round complexity of secure protocols』、Annual ACM Symposium on Theory of Computing 22、ページ503-513、1990年」にて提案した方法がある。以降この文献を非特許文献１と呼ぶ。
【０００３】
非特許文献１に開示される技術は、ネットワークで繋がるλ人の計算者u_αがそれぞれ秘密の入力x_αを持ち、任意の関数gが与えられたときに、計算者が互いに協力して関数の出力$g(x_1,\ldots,\lambda)$を計算する方法で、各計算者の秘密が$g(x_1,\ldots,x_\lambda)$以上に漏ることがなく、かつ、この計算に必要な通信回数が定数となる方法である。非特許文献1に開示される技術について図１、図２および図１９を用いて説明する。
【０００４】
［ガードブル回路］
［記法］
回路fはm個の論理ゲートで構成されるものとし、各ゲートを$G_1,\ldots,G_l,\ldots,G_m$とする。各ゲート図１９に示されるように、2入力1出力で、各出力は複数のゲートに入力されても良いものとする。G_kの出力配線は一般に複数のゲートに入力されるが、配線を流れる信号の値はどれも同じ値で0または1とする。また、このゲートG_kから出る配線を全てw_kと呼ぶ。回路fに入力される配線の本数をn個とし、これを
$\{w_k\}_{k=m+1,\ldots,m+n}$とする。$w_1,\ldots,w_l$を回路fの出力とする。
【０００５】
計算者の人数をλ、計算者の集合を
【０００６】
【数１】

$$\{u^{(\alpha)}\}_{\alpha=1,\ldots,\lambda}$$

【０００７】
とする。
【０００８】
【数２】

$$u^{(\alpha)}$$

【０００９】
が回路fへ入力するビットの個数を
【００１０】
【数３】

$$I_\alpha$$

【００１１】
個とし、それらの和をnとする
【００１２】
【数４】

$$(\Sigma_{\alpha=1}^{\lambda} I_{\alpha}=\lambda).\ k=m+1,\ldots,m+n$$

【００１３】
に関して各W_kに入力されるビットをb_kとし、それぞれのビットを
【００１４】
【数５】

$$u(\alpha)$$

【００１５】
に
【００１６】
【数６】

$$I_{\alpha}$$

【００１７】
個ずつ次のように割り振る。すなわち、
【００１８】
【数７】

$$u(\alpha)$$

【００１９】
は集合
【００２０】
【数８】

$$[\,b_k \in \{0,1\}]k=m+\Sigma_{\beta=1}^{\alpha-1} I_{\beta}+1,\ldots,m+\Sigma_{\beta=1}^{\alpha} I_{\beta}$$

【００２１】
を決定する。
【００２２】
ゲートG_kにゲートG_iとゲートG_jの出力が入力されたとき、G_jの出力b_j、G_jの出力b_j、とG_kの出力b_kの間の関係を、
【００２３】
【数９】

$$b_k = b_i \circledcirc_{G[k]} b_j$$

【００２４】
と表す。また、
【００２５】

【数１０】

□

【００２６】
はbitの排他的論理和、
【００２７】
【数１１】

【００２８】
は文字列の連結を表すとする。
【００２９】
tは安全変数で、G,H,Fはtλビットの文字列を出力する疑似乱数生成器とする。
【００３０】
[構成]
プロトコルは大きく三つの処理、(1)入力処理402、(2)多人数計算によるガーブルド回路の並列構築処理400と、(3)入力の開示と回路の計算を行う結果出力処理401とに分かれる。
【００３１】
入力処理402は次の様に行う。計算する回路に関する情報、他の計算者に関する情報、各装置の入力データを、各装置に入力する。
【００３２】
ガーブルド回路の並列構築処理400は次の様に行う。この処理の過程では、図２に示される、λ個の計算装置501が個別に計算を行うフェーズ502と、全ての計算機が互いに通信するフェーズ503が交互に繰り返し行われる。そして、この繰り返しの回数としてある定数回504が存在して、計算したい関数がどのようなものであれ以下の処理は終了できる。また、各通信フェーズでは、各計算装置がその他の全ての計算装置にデータを送信するが、この時送信するデータを生成するために、この送信と同じ通信フェーズで行われる他の計算装置の送信データを必要としてはならない。すなわち、他の計算装置のデータを待たねばできない送信があるとき、この送信を行う通信フェーズを、データを待っている通信フェーズとは別のものと数える。
【００３３】
[1]計算者は協力してtビットの文字列の集合
【００３４】
【数１２】

$$\{s\alpha_k, s'\alpha_k \in_R \{0,1\}^t\}_{k=1,\ldots,m+n;\ \alpha=1,\ldots,\lambda}$$

【００３５】
及びビットの集合
【００３６】
【数１３】

$$\{\rho_k \in_R \{0,1\}\}$$

【００３７】
を一様無作為に、計算者全員に秘密分散される様に生成する。ここで、
$S_k := s_k^1 \cdot s_k^2 \cdot \ldots \cdot s_k^\lambda$

$S'_k := s'_k{}^1 \cdot s'_k{}^2 \cdot \ldots \; s'_k{}^\lambda$
とする。$\{S_k\}, \{\rho_k\}$は
【００３８】
【数１４】

$$\lambda_k \square b_k = 0$$

【００３９】
であるならば、回路の計算フェーズにおいてS_kが公開され、
【００４０】
【数１５】

$$\lambda_k \square b_k = 1$$

【００４１】
ならばS'_kが公開されることになる。
【００４２】
[2]それぞれの計算者
【００４３】
【数１６】

$$u_\alpha$$

【００４４】
には、
【００４５】
【数１７】

$$[s_{\alpha\,k}]_{k=1,\ldots,m+n}$$

【００４６】
が明かされる。
【００４７】
[3]それぞれの計算者
【００４８】
【数１８】

$$u_\alpha$$

【００４９】
は、k=1,...,m+nに関して、それぞれtλビットの文字列である
【００５０】

【数１９】

$$g\alpha_k = G(s\alpha_k)$$

$$g'\alpha_k = G(s'\alpha_k)$$

$$h\alpha_k = H(s\alpha_k)$$

$$h'\alpha_k = H(s'\alpha_k)$$

$$f\alpha_k = F(s\alpha_k)$$

$$f'\alpha_k = F(s'\alpha_k)$$

【００５１】
を計算し、
【００５２】
【数２０】

$$[g\alpha_k, g'\alpha_k, h\alpha_k, h'\alpha_k, f\alpha_k, f'\alpha_k]_k$$

【００５３】
をコミットし、さらにこれらの値を正しく計算したことを他の計算者に証明する。
【００５４】
[4]k=m+1,...,m+nに関して、計算者達は、
【００５５】
【数２１】

$$\sigma_k{}^1 \cdot \ldots \sigma_k{}^\lambda = S_k \text{ もし } \lambda_k \square b_k = 0$$
$$\sigma_k{}^1 \cdot \ldots \sigma_k{}^\lambda = S'_k \text{ もし } \lambda_k \square b_k = 1$$

【００５６】
を秘密に分散して計算する。
【００５７】
[5]計算者達は協力してk=1,...,m+nに関して、
【００５８】

【数２２】

$A_k = g_i^1 \square \ldots \square g_i^\lambda \square g_j^1 \square \ldots \square g_j^\lambda \square S_k$ もし $\rho_i \circledcirc_{G[k]} \rho_j = \rho_k$

$A_k = g_i^1 \square \ldots \square g_i^\lambda \square g_j^1 \square \ldots \square g_j^\lambda \square S'_k$ もし $\rho_i \circledcirc_{G[k]} \rho_j \neq \rho_k$

$B_k = h_i^1 \square \ldots \square h_i^\lambda \square g'^1_j \square \ldots \square g'^\lambda_j \square S_k$ もし $\rho_i \circledcirc_{G[k]} \rho'_j = \rho_k$

$B_k = h_i^1 \square \ldots \square h_i^\lambda \square g'^1_j \square \ldots \square g'^\lambda_j \square S'_k$ もし $\rho_i \circledcirc_{G[k]} \rho'_j \neq \rho_k$

$C_k = g'^1_i \square \ldots \square g'^\lambda_i \square h_j^1 \square \ldots \square h_j^\lambda \square S_k$ もし $\rho'_i \circledcirc_{G[k]} \rho_j = \rho_k$

$C_k = g'^1_i \square \ldots \square g'^\lambda_i \square h_j^1 \square \ldots \square h_j^\lambda \square S'_k$ もし $\rho'_i \circledcirc_{G[k]} \rho_j \neq \rho_k$

$D_k = h'^1_i \square \ldots \square h'^\lambda_i \square g'^1_j \square \ldots \square g'^\lambda_j \square S_k$ もし $\rho'_i \circledcirc_{G[k]} \rho'_j = \rho_k$

$D_k = h'^1_i \square \ldots \square h'^\lambda_i \square g'^1_j \square \ldots \square g'^\lambda_j \square S'_k$ もし $\rho'_i \circledcirc_{G[k]} \rho'_j \neq \rho_k$

【００５９】
を秘密に分散して計算する。但しゲートG_kに入力される信号はゲートG_iとゲートG_jの出力とする。この様子を図19に示す。結果出力処理401における入力の開示と回路の生成は次の様に行う。

【００６０】
[1]計算者は

【００６１】
【数２３】

$$\{\rho_k\}_{k=1,\ldots,l}$$

$$\{f_k^\alpha\}_{k=1,\ldots,m+n;\,\alpha=1,\ldots,\lambda}$$

$$\{\sigma_k^1 \cdot \ldots \cdot \sigma_k^\lambda\}_{k=1,\ldots,m+n}$$

$$\{A_k, B_k, C_k, D_k\}\}_{k=1,\ldots,m+n}$$

【００６２】
を公開する。

【００６３】
[2]回路の入力ににより近いkから順番にk=1,...,m+n に関して、S_iまたはS'_i、及びS_j、または、S'_jから、次のようにしてS^*_kを得る。これはS_kまたはS'_kである。

【００６４】

【数２４】

$S_k^* = A_k \square g_i^1 \square \ldots \square g_i^\lambda \square g_j^1 \square \ldots \square g_j^\lambda$ もし S_i, S_j を持っているなら.

$S_k^* = B_k \square h_i^1 \square \ldots \square h_i^\lambda \square g'^1_j \square \ldots \square g'^\lambda_j$ もし S_i, S'_j を持っているなら.

$S_k^* = C_k \square g'^1_i \square \ldots \square g'^\lambda_i \square h_j^1 \square \ldots \square h_j^\lambda$ もし S'_i, S_j を持っているなら.

$S_k^* = D_k \square h'^1_i \square \ldots \square h'^\lambda_i \square g'^1_j \square \ldots \square g'^\lambda_j$ もし S'_i, S'_j を持っているなら.

【００６５】

[3]全ての $\alpha = 1, \ldots, \lambda$; $k = 1, \ldots, m+n$ に関して

【００６６】

【数２５】

$$f^{\alpha}{}_k = F(s^{\alpha}{}_k),$$

$$f'^{\alpha}{}_k = F(s'^{\alpha}{}_k)$$

【００６７】

を確認することで、

$S^*{}_k = S_k$ または $S^*{}_k = S'{}_k$ を確認する。

【００６８】

[4]全ての計算者はk=1,...,1に関して、S_k を手にいれた場合は $\rho_k + b_k = 0$、S'_k を手にいれた場合は $\rho_k + b_k = 1$ が成り立つことより、b_k を求める。

【００６９】

技術分野の欄に記述された様な方法のその他の従来の技術として、Ishai、Kushilevitzは、文献「Y. Ishai and E. Kushilevitz、『Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation』、IEEE Symposium on Foundations of Computer Science 2000、ページ294-304」にて提案した方法がある。以降この文献を非特許文献２と呼ぶ。非特許文献２の従来の技術を図３および図４を用いて説明する。

【００７０】

[ランダマイジング多項式]

非特許文献２には、与えられた関数をある有限体上の低い次数の多項式で表現する方法が提案されている。特に任意の関数が次数３の多項式で表現可能であることが示されている。次数が低い多項式を評価することは定数回のラウンドで可能である。一般に関数は、回路等様々な形で表現することができる。

【００７１】

次にあげるブランチング問題も一般の関数を表現することができる。ブランチング問題BP=(G, ϕ、s,t)をmod-pブランチング問題と呼ぶ。G=(V,E)は向き付けられたグラフ、ϕはラベル付け関数で、Gのそれぞれの辺に、1、$x^1{}_i$、あるいはその否定$x^0{}_i$のいずれかを関係付けるもの、s,tは特別な頂点である。

【００７２】

入力$x=(x_1, \ldots, x_n)$が与えられたとき、ラベル付け関数ϕによりGの部分グラフG_xが与えられる。BPで計算されるboolean関数fの値は、G_xにおけるs-tを結ぶ経路の数をpで割った余りが0ならばf(x)=0、そうでなければf(x)=1とする。BPの大きさをGの頂点の数とする。

【００７３】
BPの大きさをlとする。部分グラフG_xのl¥timesl隣接行列をH_xとすると、s-t間を結ぶ経路の数は、
【００７４】
【数２６】

$$(I+H_x+H_x^{2}+\cdots)_{st} = ((1-H_x)^{-1})_{st} \bmod p$$

$$=\det M_x / \det(I-H_x)] \bmod p$$

【００７５】
となる。ここでM_xは行列$(I-H_x)$からs行とt列を除いた行列とする。
よって、
【００７６】
【数２７】

$$f(x)=0 \Leftrightarrow \mathrm{rank}(M_x) = l-1$$

$$f(x)=1 \Leftrightarrow \mathrm{rank}(M_x) = l$$

【００７７】
となる。また、M_xはxに関して高々1次の成分からなる。
【００７８】
[計算方法]
ブール関数fが与えられ、その入力xが複数の計算者に分配されている時に、ランダマイジング多項式の方法を用いてf(x)を求める方法を記す。
【００７９】
図３に示すように、
[1]計算する関数に関する情報、他の計算者に関する情報、各装置の入力データを、各装置に入力する（605）。
【００８０】
[2]fに対応するBPを構成する（600）。
【００８１】
[3]次の処理を十分な回数並列して行う（601）。
【００８２】
[処理]
図４に示すように、
全ての計算者は各成分を分散してlxl行列R_1,R_2を一様無作為に生成し（603）、3行列R_1,M_x,R_2の積である$R_1 M_x R_2$を計算する（604）。
【００８３】
各成分はR_1,R_2,xの要素の高々3次の式であり、その計算に必要なラウンド数は高々定数回である。
【００８４】
[4]全ての$\mathrm{rank}R_1 M_x R_2$の値からM_xのrankがlであるかを推測し、lである確率が高ければ1を、でなければ0を出力する（602）。
【００８５】
上記方法において、$\mathrm{rank}(M_x)=\mathrm{rank}(M'_x)$であれば、$R_1 M_x R_2$と$R_1 M'_x R_2$の分布は同じになるので、xに関する情報はf(x)以外は新たに漏ることはない。

【００８６】
さらに、いかなるlに対しても、rank(M_x)=1であるならばrank($R_1 M_x R_2$)=1となる確率は0.08より大きいため、項目2の処理を実行する回数はlに依存しない。
【００８７】
[計算量と通信量]
ガーブルド回路を用いた方法では、各ゲートに関する計算は独立して行われ、全体の通信量と計算量はゲートの数に比例する。t-n閾値分散($2t^2$に比例する。t-n閾値分散での計算とはn人で秘密を分散して計算を行うが、このうちt人が各自知っているデータを持ち寄らない限り、分散された秘密や計算の途中の意味のあるデータを知ることができない計算方法である。
【００８８】
ランダマイジング多項式を用いた方法では、t-n閾値分散が行われた場合で、
【００８９】
【数２８】

$$t^2$$

【００９０】
とBPの大きさの2乗に比例し、ラウンド数は2(3)となる。
【００９１】
ランダマイジング多項式の方法では通信量と計算量はゲート数の高々1次に比例する。さらに、最高次の係数はランダマイジング多項式の方法のものが断然低く、効率的である。
【００９２】
しかし、ここではt-n閾値分散でt>n/2である様な場合で第三者が計算の正当性を検証できることを要求する場合に特に注目する。この様な場合に前述の方法を拡張することは容自明である。拡張の結果は、ガーブルド回路を用いた方法で全体の通信量と計算量はゲートの数とt^3に比例し、ランダマイジング多項式の方法を用いた場合、通信量と計算量がゲート数の1.5乗に比例し、ゲート数が大きい場合効率的ではない。
【非特許文献１】D. Beaver、S. Micali、and P. Rogaway、『The round complexity of secure protocols』、Annual ACM Symposium on Theory of Computing 22、ページ503-513、1990年
【非特許文献２】Y. Ishai and E. Kushilevitz、『Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation』、IEEE Symposium on Foundations of Computer Science 2000、ページ294-304
【発明の開示】
【発明が解決しようとする課題】
【００９３】
第１の問題点は、非特許文献1の方法は、各計算者の計算量及び計算の正当性を検証する検証者の計算量が膨大になるということである。
【００９４】
その理由は、各計算者は疑似乱数生成装置の出力を計算しなければならないが、この計算を正しく行ったことを計算結果を隠したまま証明する必要があるためである。
【００９５】
第２の問題点は、非特許文献2の方法も、やはり各計算者の計算量及び計算の正当性を検証する検証者の計算量が膨大になるということである。
【００９６】
その理由は、各計算者が計算する計算量が、関数を回路で表現した場合のゲート数の1.

5乗に比例し、かつ多くの場合ゲート数は非常に多いため、全体の計算量が膨大になると言うことである。

【００９７】

本発明の目的は、回路を表現するゲート数が多くなってもその計算装置がゲート数に比例するに留め、計算装置がその計算の正当性を証明すべき疑似乱数生成装置の出力を計算する必要がなく、かつ計算装置の通信回数が関数に依らずに定数回となる計算方法およびシステムを提供することにある。

【課題を解決するための手段】

【００９８】

本発明の計算方法は、複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

出力処理とからなり、

前記入力処理では、前記複数の計算装置に、回路と、前記回路への入力ビットとが入力され、

まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする。

【００９９】

本発明の他の形態による計算方法は、複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

ElGamal暗号文準備処理と、

逐次置換再暗号処理と、

結果出力処理とからなり、

前記入力処理は、

前記複数の計算装置に複数のゲートから構成された回路の情報及び前記複数の計算装置に関する情報が入力される、情報入力ステップと、

関数の入力データを複数に計算装置の個数に分散したデータである複数の部分データを、それぞれの計算装置にそれぞれ一つずつ入力する分散入力ステップと、

からなり、

前記ElGamal暗号文準備処理は、

少なくとも一つの計算装置が、与えられた関数を実現する回路のゲートに対応したElGamal暗号文の集合を生成するElGamal暗号文準備ステップとからなり、

前記逐次置換再暗号処理は、

置換再暗号処理を各計算装置が順番に行う処理で、前記置換再暗号処理は、順番が回ってきた計算装置が、一つ前の順番に対応する計算装置からElGamal暗号文の集合を受け取る暗号文取得ステップと、

前記暗号文取得ステップにて受け取った暗号文の集合を順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化ステップと、

前記暗号文の置換と再暗号化ステップで生成したデータを、少なくとも次の順番の計算装置に公開するステップと、

からなり、

前記結果出力処理は、

前記逐次置換再暗号処理で生成された暗号文の一部を復号あるいは部分復号する部分復号ステップと、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデー

タを暗号化している暗号文を復号する復号ステップと、
前記復号ステップで復号されたデータと、前記部分復号ステップで部分復号されたデータを用いて、回路の出力を評価する回路の評価ステップと、
からなることを特徴とする。
【０１００】
この場合、前記各ゲートに対応するElGamal暗号文の集合は、前記各計算装置が各ゲートに対応して生成した秘密鍵のElGamal暗号文の集合であり、
前記ElGamal暗号文を生成するのに用いた公開鍵は、このゲートに入力される二つの信号を生成するゲートに対応する公開鍵の和であることとしてもよい。
【０１０１】
また、前記入力処理として、各計算装置にElGamal暗号方式の領域変数を入力するステップが行なわれ、
前記ElGamal暗号文準備処理として、各前記計算装置が、各前記回路の各ゲートに対応して、ElGamal暗号文の秘密鍵を生成するゲート秘密鍵生成ステップが行なわれ、
各計算装置では、
前記ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応するゲート公開鍵を生成するゲート公開鍵の生成ステップと、
前記ゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成するゲート公開鍵の正当性の証明生成ステップと、
前記ゲート公開鍵の正当性の証明生成ステップにて生成したゲート公開鍵の正当性の証明を公開するゲート公開鍵の正当性の証明公開ステップと、
各前記回路のゲートで回路への入力が直接入力されるゲートに対応して、ElGamal暗号文の秘密鍵を生成する入力のゲート秘密鍵の生成ステップと、
前記入力ゲート秘密鍵の生成ステップにて生成した秘密鍵に対応する入力ゲート公開鍵を生成する入力のゲート公開鍵の生成ステップと、
前記入力のゲート公開鍵の生成ステップにて生成した公開鍵の正当性の証明を生成する入力のゲート公開鍵の正当性の証明生成ステップと、
前記入力のゲート公開鍵の正当性の証明生成ステップにて生成し入力の公開鍵の正当性の証明を公開する入力のゲート公開鍵の正当性の証明公開ステップと、
その他の各計算装置が生成して公開したゲート公開鍵を取得するゲート公開鍵取得ステップと、
前記ゲート公開鍵取得ステップにおいて取得したゲート公開鍵を統合するゲート公開鍵の統合ステップと、
前記ゲート公開鍵の統合ステップにおいて統合したゲート公開鍵により、この計算装置が生成したゲート秘密鍵を暗号化するゲート秘密鍵の暗号化ステップと、
前記ゲート秘密鍵の暗号化ステップにおいて生成したゲート秘密鍵の暗号文を公開するゲート秘密鍵の暗号文の公開ステップと、
前記ゲート秘密鍵の暗号文の正当性証明を生成するゲート秘密鍵の暗号文の正当性の証明生成ステップと、
前記ゲート秘密鍵の暗号文の正当性の証明生成ステップにおいて生成したゲート秘密鍵の暗号文の正当性の証明を公開するゲート秘密鍵の暗号文の正当性の証明公開ステップと、
各計算装置に入力された回路の入力の部分に対応する暗号文を生成する入力の暗号文生成ステップと、
前記入力の暗号文生成ステップにて生成した回路の入力の部分に対応する暗号文の正当性の証明を生成する入力の暗号文の正当性の証明生成ステップと、
前記入力の暗号文の正当性の証明生成ステップにおいて生成した証明を公開する入力の暗号文の正当性の証明公開ステップと、
出力のゲートに対応する暗号文を生成して公開する出力の暗号文の生成ステップと、
を含み、

前記置換再暗号処理が、
前記ゲート秘密鍵の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化するゲート秘密鍵の暗号文の置換と再暗号化ステップと、
前記入力の暗号文の集合の順番をあらかじめ決められた許された置換の方法から無作為に一つの置換を選んで入れ替えて再暗号化する入力の暗号文の置換と再暗号化ステップと、
前記出力の暗号文の集合の順番をあらかじめ決められた許された置換方法から無作為に一つの置換を選んで入れ替えて再暗号化する出力の暗号文の置換と再暗号化ステップと、
前記ゲート秘密鍵の暗号文の置換と再暗号化ステップと入力の暗号文の置換と再暗号化ステップと出力の暗号文の置換と再暗号化ステップとにおいてなされた置換と再暗号化の正当性の証明を生成し公開するゲート秘密鍵の暗号文と入力の暗号文と出力の暗号文の置換と再暗号化の正当性の証明生成と公開ステップと、
を含み、
前記結果出力処理の部分復号ステップが、
前記計算装置が互いに通信及び計算することで前記ゲート秘密鍵の暗号文を部分復号するゲート秘密鍵の部分復号ステップと、
前記計算装置が互いに通信及び計算することで前記入力の暗号文を部分復号する入力の暗号文の部分復号ステップと、
前記計算装置が互いに通信及び計算することで前記出力の暗号文を部分復号する出力の暗号文の部分復号ステップと、
前記ゲート秘密鍵の部分復号ステップと入力の暗号文の部分復号ステップと出力の暗号文の部分復号ステップとでなされた部分復号の正当性の証明を生成し公開するゲート秘密鍵と入力の暗号文と出力の暗号文の部分復号ステップの正当性の証明生成と公開ステップと、
を含み、
他の計算装置の公開した種々の正当性の証明を検証するステップを含む、
こととしてもよい。

【０１０２】

本発明の計算システムは、複数の計算装置と、
複数の計算装置と通信する手段と、
入力処理手段と、
ElGamal暗号文準備手段と、
置換再暗号処理手段と、
結果出力処理手段と、
からなる関数を評価する計算システムであって、
前記入力処理手段は、出力を求めたい回路の情報と、前記複数の計算装置に関する情報と、前記複数の計算装置がそれぞれ前記回路の入力のどの部分を所持しているかという情報と、を入力し、
前記ElGamal暗号文準備処理手段は、与えられた関数を実現する回路のゲートに対応したElGamal暗号文の集合を生成するElGamal暗号文を準備し、
前記置換再暗号処理手段は、
順番が回ってきた計算装置が、一つ前の順番に対応する計算装置からElGamal暗号文の集合を受け取る暗号文取得手段と、
前記暗号文取得手段により受け取られた暗号文の集合の順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化手段と、
前記暗号文の置換と再暗号化手段を用いて生成したデータを、少なくとも次の順番の計算装置に公開する手段と、
からなり、
前記結果出力手段は、

置換再暗号処理手段で生成された暗号文の一部を復号あるいは部分復号する部分復号手段と、
前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文の自分に関する暗号化を復号する復号手段と、
前記複数の計算機が前記復号手段で復号したデータと前記複数の計算機が前記部分復号手段で部分復号されたデータを用いて回路の出力を評価する回路の評価手段と、
からなることを特徴とする。
【０１０３】
本発明の他の形態による計算システムは、複数の計算装置、入力手段、出力手段を含み、まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す計算システムであって、
前記入力手段では前記計算装置に回路の情報と、前記回路への入力ビットの一部とが入力され、
第ゼロ周目の計算は第一の計算装置が第一周目の計算を行う前に行い、
前記複数の計算装置には、
前記各周の計算に使用される送られてきたデータを取得するデータ取得手段と、正当性証明検証手段と、署名文検証手段と、第一の計算装置のみが行う第一計算装置特別計算手段と、乱数生成を行う乱数生成手段と、本計算を行う本計算計算手段と、本計算で行った計算の正当性を証明する正当性証明作成手段と、署名手段とデータ送信手段とからなり、
前記送られてきたデータは、別の計算装置から送られてきたデータと、データ本体と、データ本体に対する正当性証明と、署名文とからなり、
前記署名文は、前記別の計算装置から送られてきたデータと、前記データ本体と、前記データ本体に対する正当性証明との組に対する署名文であるようなデータで、
前記正当性証明検証手段は前記送られてきたデータ中の正当性証明を検証し、
前記署名検証手段は、前記送られてきたデータ中署名文を検証し、
前記本計算は前記乱数生成手段で生成された乱数を用いて計算し、
前記署名手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明との組に対する署名文を作成し、
前記データ送信手段が、前記送られてきたデータと、前記本計算で計算された計算結果であるデータ本体と、前記正当性証明作成手段で作成された正当性証明と前記署名手段で作成された署名文との組を送信する事を特徴とする。
【０１０４】
この場合、前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第一周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であるとしてもよい。
【０１０５】
また、各周の計算が、第一周目の計算手段と、第一周目以降の周の計算手段とからなり、
前記計算手段は、第ゼロ周目の計算手段では真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組を作成し、前記第一周目の計算手段が再暗号に使用する為の公開鍵を作成する再暗号用公開鍵作成手段と、送られてきたデータを変換するデータ変換手段と、秘密鍵変換手段と、乱数変換手段とからなり、
前記データ変換手段が、前記データ本体である暗号文の組を、真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる別の組

に変換する為の手段であり、
前記秘密鍵変換手段が、前記データ変換手段の計算結果である暗号文達の組に使用されている秘密鍵を再暗号用公開鍵作成手段で作成された公開鍵に対応する秘密鍵に変換する手段であり、
前記秘密鍵変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、
前記乱数変換手段が前記データ変換手段の計算結果である暗号文達の組に使用されている乱数を変換する手段であり、
前記乱数変換手段の計算結果が真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であるとしてもよい。
【０１０６】
また、第一周目以降の周の計算手段が、第二周目の計算手段と第二周目以降の計算手段とからなり、
前記送られてきたデータのデータ本体と前記本計算で計算されたデータ本体とが、第二周目の計算では、共に真理値群環上の多重配列エルガマル暗号文達と真理値群環上の拡張多重配列エルガマル暗号文達とからなる組であり、
前記第二周目の計算手段が、
前記送られてきたデータの前記データ本体を変換してエルガマル暗号文もしくは楕円曲線エルガマル暗号文を作成する暗号変換手段と、前記送られてきたデータのデータ本体の暗号文達を部分復号する部分復号手段とからなるとしてもよい。
【０１０７】
さらに、第二周目以降の計算手段が、第三周目の計算手段のみからなり、第三周目の計算手段の前記本計算手段が、前記送られてきたデータをそのまま出力し、
前記正当性証明作成手段が空列を出力するとしてもよい。
【０１０８】
本発明の多数の入力から関数を計算する方法は、ElGamal暗号方式を利用して、その値を隠したゲートの入出力の対応表を生成する手段とを備え、各入力を持った装置が次々と順番に、図５に示すようにElGamal暗号文の集合からなる対応表の順番を入れ替えるよう動作する。このような構成を採用し、各装置に分配された入力に対する関数の出力を計算することにより本発明の目的を達成することができる。
【発明の効果】
【０１０９】
第１の効果は、各計算装置の計算量と通信量が回路のゲート数に比例するに留まり、効率的であることにある。
【０１１０】
その理由は、各ゲート毎にゲートの入出力の対応表をElGamal暗号文で生成し、疑似乱数生成装置を用いなかったため、この対応表の計算の正当性を第三者に証明するのが容易になったためである。
【０１１１】
第２の効果は、各計算装置の他の計算装置との通信回数が、計算する回路のゲート数に依らず定数回に留まり、効率的であることにある。
【０１１２】
その理由は、各ゲートの入出力の対応表の対応関係がいずれの計算装置にも分からなくなる操作が必要であるが、この操作が各計算装置が順番に対応関係を入れ替える操作を行えば実現されるからである。
【発明を実施するための最良の形態】
【０１１３】
次に、本発明の実施例について図面を参照して説明する。
【０１１４】
実施例１

本発明の第１の実施例について、図６ないし図１３を用いて説明する。

【０１１５】

[準備]

[システム構成]

図１１に示すように、計算装置308がλ個あり、それぞれ通信手段307を備えている。以下ではこの計算機を順番に、

【０１１６】

【数２９】

$$\{u^{(\alpha)}\}_{\alpha=1,\ldots,\lambda}$$

【０１１７】

と呼ぶことにする。計算装置数、各計算装置と対応する添字αとの関係等をシステムの構成情報と呼ぶ。

【０１１８】

[回路の情報]

後の説明で、回路の情報が各計算装置

【０１１９】

【数３０】

$$\{u^{(\alpha)}\}_{\alpha=1,\ldots,\lambda}$$

【０１２０】

に入力されるが、この回路の情報を説明する。

【０１２１】

まず、入力される回路の情報が表現する回路をfと呼ぶことにする。fはm個の論理ゲートで構成されている回路とする。各ゲートを$G_1,\ldots,G_l,\ldots,G_m$と呼ぶ。ここでは各ゲートは2入力1出力であるとする。この様なゲートで回路が構成されていなかった場合は、各ゲートを複数の2入力1出力のゲートからなる等価な回路に置き換える。この置き換え方法は明らかなので省略する。また回路のあるゲートから他のゲートの入力へ信号を送る配線は、0または1に対応する信号を送るとする。G「k」の出力配線を$w_{[k]}$とする。fに入力される配線の本数をn個とし、これを$\{w_{[k]}\}_{k=m+1,\ldots,m+n}$とする。配線は途中で分岐して二つ以上のゲートに入力していても良い。配線$_{[k]}$は分岐しても同じ信号を送信するものとし、この分岐した配線をまとめて$w_{[k]}$と呼ぶ。$w_{[1]},\ldots,w_{[l]}$を回路fの出力とする。回路の配線は全て、ゲートの出力配線か回路への入力配線のいずれかであるので、配線全て$\{w_{[k]}\}_{k=1,\ldots,m+n}$が配線の全てである。

【０１２２】

ゲートG_kにゲートG_iとゲートG_jの出力が入力されたとき、すなわち、配線$w_{[i]}$と配線$w_{[j]}$がゲートG_kに入力され、配線w_kがG_kの出力のための配線として繋がっているときに、G_iの出力b「i」、G_jの出力b「j」、とG_kの出力b「k」の間の関係を、

【０１２３】

【数３１】

$$b\lceil k\rfloor = b\lceil i\rfloor \circledcirc_{G\lceil k\rfloor} b\lceil j\rfloor$$

【０１２４】

とし、各計算装置

【０１２５】

【数３２】

$$u(\alpha)$$

【０１２６】
は、fに入力する信号の一部を持っているものとする。すなわち、配線{w〔k〕}k=m+1,...,m+nのうちの一部に伝搬させる信号を知っているとする。
【０１２７】
【数３３】

$$u(\alpha)$$

【０１２８】
がfへ入力するビットの個数を
【０１２９】
【数３４】

$$I_\alpha$$

【０１３０】
個とし、全ての計算装置の持つ入力を集めると、回路への入力全てとなるとする。すなわち、
【０１３１】
【数３５】

$$\Sigma_{\alpha=1}^{\lambda} I_\alpha = \lambda$$

【０１３２】
となる。k=m+1,...,m+nに関して各w〔k〕に入力されるビットをb「k」とし、それぞれのビットを
【０１３３】
【数３６】

$$u(\alpha)$$

【０１３４】
に
【０１３５】
【数３７】

$$I_\alpha$$

【０１３６】
個ずつ次のように割り振る。すなわち、
【０１３７】
【数３８】

$$u(\alpha)$$

【０１３８】

は集合

【０１３９】

【数３９】

$$\{b\lceil k\rfloor \in \{0,1\}\}k=m+\Sigma_{\beta=1}^{\alpha-1} I_\beta +1,\ldots,m+\Sigma_{\beta=1}^{\alpha} I_\beta$$

【０１４０】

を決定する。ゲートの番号の割り振りを変更しても回路は本質的に変わらないため、上記のように入力を割り振っても一般性は損なわれない。

【０１４１】

上記m個のゲート$G_1,\ldots,G_m$、それぞれのゲートの行う演算

【０１４２】

【数４０】

$$\circledcirc_{G\lceil k\rfloor},$$

【０１４３】

、それぞれのゲートに繋がる配線$\{W\lceil k\rfloor\}_{k=m+1,\ldots,m+n}$,入力配線の計算装置に対する割り振り

【０１４４】

【数４１】

$$\{I_\alpha\}_{\alpha=1,\ldots,\lambda}$$

【０１４５】

を回路の情報300と呼ぶ。

【０１４６】

[演算に用いる群]

本実施例では、楕円曲線上での演算を利用するのでこれを説明する。しかし、これは本発明を実施するためにはこれは必ずしも必須ではない。これに代替となるものとして、素体上の演算等、可換な乗法群であれば良い。

【０１４７】

以降、Eを位数が素数qである楕円曲線、0をEの無限遠点、G(≠0)をE上の点とする。qは、暗号学的に安全とされるに十分な大きさであるとする。楕円曲線E上の点からZ/qZ上への写像をϕとする。ϕは、その像の空間が十分に大きいものを選ぶ。ϕの例として、楕円曲線E上の点の座標の片方の値を使う等がある。hをZ/qZの要素、Gを楕円曲線上の点としたとき、Gのh倍点を[h]Gと表す。

【０１４８】

[記法]

文字の右肩に記された文字は上付きの添字であって、冪乗を表す指数ではない。また、□はbitの排他的論理和を表すとする。

【０１４９】

[入力処理203,312]

処理が開始されると、図６に示されるように、まず、入力処理２０３が行なわれる。この入力処理２０３について、処理を詳細に示す図１２および図１３を参照して説明する。

【０１５０】

ElGamal暗号文準備処理では情報公開手段と公開情報取得手段を使って、データの公開と取得の両方を行う（309）。

【０１５１】

[領域変数の決定]

計算はE,G及びϕを決定する。また、ハッシュ関数を利用する等の方法で、誰もがH=[h]GなるZ/qZの元hが分らない様な楕円曲線上の点Hを決定する。これらの値E,G,H,ϕを領域変数301と呼ぶ。これらはあらかじめ全ての計算装置に格納しておく（図１３の100）。

【０１５２】

[回路の情報及び、回路の部分入力の入力]

回路fの情報及びシステムの構成情報が全ての計算装置に入力される（図１３の101）。

【０１５３】

各計算装置

【０１５４】

【数４２】

$$\{u(\alpha)\}_{\alpha=1,\ldots,\lambda}$$

【０１５５】

それぞれに、回路への分散された部分入力

【０１５６】

【数４３】

$$\{b\lceil k\rfloor \in \{0,1\}\}_{k=m+\sum_{\beta=1}^{\alpha-1} I_\beta+1,\ldots,m+\sum_{\beta=1}^{\alpha} I_\beta}$$

【０１５７】

を入力する（図１３の102）。

【０１５８】

[ElGamal暗号文準備処理200,303]

[ゲート毎の秘密鍵と公開鍵設定]

次に、図６に示されるように、ElGamal暗号文準備処理２００が行なわれる。このElGamal暗号文準備処理２００について、処理を詳細に示す図７および図８を参照して説明する。

【０１５９】

各計算装置

【０１６０】

【数４４】

$$u(\alpha)$$

【０１６１】

は、全てのk=1,...,m+n、全ての

【０１６２】

【数４５】

$$b \in \{0,1\}$$

【０１６３】

に関して、ゲート秘密鍵

【０１６４】

【数４６】

$$X(\alpha)b_{[k]} \in_R E$$

$$z(\alpha) \in_R Z/qZ$$

【０１６５】
を一様無作為に生成し（図７の103）、
全てのk=1,...,m+n、全ての
【０１６６】
【数４７】

$$b \in \{0,1\}$$

【０１６７】
に関して，
【０１６８】
【数４８】

$$x(\alpha)b_{[k]} = \phi(X(\alpha)b_{[k]})$$

【０１６９】
を生成し、
全てのk=1,...,m+n、全ての
【０１７０】
【数４９】

$$b \in \{0,1\}$$

【０１７１】
に関して、ゲート公開鍵
【０１７２】
【数５０】

$$Y(\alpha)b_{[k]} = [x(\alpha)b_{[k]}]G$$

$$Z(\alpha) = [z(\alpha)]G$$

【０１７３】
を生成し（図７の104）、各計算装置
【０１７４】
【数５１】

$$u_\alpha$$

【０１７５】
は各自の生成したゲート公開鍵をそれぞれ、情報公開装置を用いて公開する（図７における105）。以降本実施例1では公開するとは、情報公開装置を用いて公開することである。

【０１７６】
併せて計算装置
【０１７７】
【数５２】

$$u_{\alpha} \text{ は, 各 } Y(\alpha)b_{[k]}, Z(\alpha) \text{に関して} x(\alpha)b_{[k]}, z(\alpha)$$

【０１７８】
の知識の証明を、別記述Aの方法に従って、ゲート公開鍵の正当性証明として生成（図７における106）し、公開（図７の107）する。
【０１７９】
［入力の公開鍵設定］
各計算装置
【０１８０】
【数５３】

$$u(\alpha)$$

【０１８１】
は、全ての
【０１８２】
【数５４】

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1} I_{\beta}, \ldots, m+\Sigma_{\beta=1}^{\alpha} I_{\beta}$$

【０１８３】
に関して、入力された
【０１８４】
【数５５】

$$b\lceil k \rfloor \in \{0,1\}$$

【０１８５】
を用いて入力ゲートの秘密鍵
【０１８６】
【数５６】

$$x^{\sim b\lceil k \rfloor}{}_{[k]} \in_R Z/qZ$$

【０１８７】
を一様無作為に生成し（図７の108）、入力ゲートの公開鍵
【０１８８】
【数５７】

$$Y^{\sim b\lceil k \rfloor}{}_{[k]} = [x^{\sim b\lceil k \rfloor}{}_{[k]}]G$$

$$Y^{\sim b\lceil k \rfloor} \square 1_{[k]} = H - Y^{\sim b\lceil k \rfloor}{}_{[k]}$$

【０１８９】

を生成し（図７の109）、
全ての
【０１９０】
【数５８】

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1} I_\beta,\ldots,m+\Sigma_{\beta=1}^{\alpha} I_\beta$$

【０１９１】
全ての
【０１９２】
【数５９】

$$b \in \{0,1\} \text{に関して}, Y^{\sim b}_{[k]}$$

【０１９３】
$b\in\{0,1\}$に関して、$Y^{\sim b}_{[k]}$
を各計算装置の入力ゲートの公開鍵として公開する（図７の110）。
【０１９４】
併せて、計算装置
【０１９５】
【数６０】

$$u_\alpha$$

【０１９６】
は、各kに関して、b「k」=0、または、b「k」=1に対して、
【０１９７】
【数６１】

$$Y^{\sim b\lceil k\rfloor}_{[k]} = [x^{\sim b\lceil k\rfloor}_{[k]}]G \text{ なる} x^{\sim b\lceil k\rfloor}_{[k]}$$

【０１９８】
の知識を持っていることの証明を、別記述Bの方法に従って、入力ゲートの公開鍵の正当性証明として生成（図７の111）し、公開する（図７の112）。
【０１９９】
［ゲートに関する処理］
全ての計算装置
【０２００】
【数６２】

$$\{u_\alpha\}$$

【０２０１】
は、公開情報取得手段を用いて、ゲート公開鍵
【０２０２】
【数６３】

$$\{Y(\alpha)b_{[k]}, Z(\alpha)\}_{\alpha=1,\ldots,\lambda}$$

【０２０３】

を取得する（図８の113）。
全てのk=1,...,mと全ての
【０２０４】
【数６４】

$$b \in \{0,1\}$$

【０２０５】
に関して、各自統合したゲート公開鍵
【０２０６】
【数６５】

$$Y^{b}_{[k]} = \Sigma_{\alpha=1} \lambda \, Y(\alpha)^{b}_{[k]}$$

$$Z = \Sigma_{\alpha=1} \lambda \, Z(\alpha)$$

【０２０７】
を生成する（図８の114）。
【０２０８】
全ての計算装置
【０２０９】
【数６６】

$$\{u_{\alpha}\}$$

【０２１０】
は、全てのk=1,...,m、全ての
【０２１１】
【数６７】

$$\varepsilon \in \{0,1\}$$

【０２１２】
に関して、
【０２１３】
【数６８】

$$r(\alpha)\varepsilon_{k} \in_{R} Z/qZ$$

【０２１４】
を一様無作為に生成して、全てのk=1,...,m、全ての
【０２１５】
【数６９】

$$b,c,\varepsilon \in \{0,1\}$$

【０２１６】
に関して、楕円ElGamal暗号方式にて暗号化することで、ゲート秘密鍵の暗号文
【０２１７】

【数７０】

$$(C^{(\alpha)bc\,\varepsilon}{}_{[k]},\ D^{(\alpha)bc\,\varepsilon}{}_{[k]}) = ([r^{(\alpha)\varepsilon}{}_{[k]}]G,\ X^{(\alpha)\varepsilon}{}_{[k]}+[r^{(\alpha)\varepsilon}{}_{[k]}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z))$$

【０２１８】
を生成し（図８の115）、これらを公開する（図８の116）。但し、ゲートG〔k〕には配線w〔i〕とw〔j〕が入力されるとする。
【０２１９】
併せて、それぞれのkに関して、全ての
【０２２０】
【数７１】

$$b,c \in \{0,1\}$$

【０２２１】
に関して、楕円ElGamal暗号文
【０２２２】
【数７２】

$$(C^{(\alpha)bc\,0}{}_{[k]},D^{(\alpha)bc\,0}{}_{[k]})$$

【０２２３】
の復号結果が同じになること、
それぞれのkに関して、全ての
【０２２４】
【数７３】

$$b,c \in \{0,1\}$$

【０２２５】
に関して、楕円ElGamal暗号文
【０２２６】
【数７４】

$$(C^{(\alpha)bc\,1}{}_{[k]},D^{(\alpha)bc\,1}{}_{[k]})$$

【０２２７】
の復号結果が同じになることの証明を、別記述Cの方法を用いて、ゲート秘密鍵の暗号文の正当性証明として生成し（図８の117）、公開する（図８の118）。
【０２２８】
全ての計算装置
【０２２９】
【数７５】

$$\{u_{\alpha}\}$$

【０２３０】
は各自、全てk=1,...,m、全ての
【０２３１】

【数７６】

$$b,c,\mu,\nu,\xi \in [0,1]$$

【０２３２】
に関して、秘密鍵識別データ暗号文
【０２３３】
【数７７】

$$(A^{(0)bc}{}_{[k]\mu,\nu,\xi}, B^{(0)bc}{}_{[k]\mu,\nu,\xi}) = (O, [\varepsilon]G)$$

$$\{(C^{(0)\alpha bc}{}_{[k]\mu,\nu,\xi}, D^{(0)\alpha bc}{}_{[k]\mu,\nu,\xi})\}_{\alpha=1,\ldots,\lambda} = \{(C^{(\alpha)bc}{}_{\varepsilon[k]}, D^{(\alpha)bc}{}_{\varepsilon[k]})\}_{\alpha=1,\ldots,\lambda}$$

【０２３４】
を生成する（図８の119）。但し、
【０２３５】
【数７８】

$$\varepsilon = ((b \square \mu) \circledcirc_{G\Gamma k]} (c \square \nu)) \square \xi$$

【０２３６】
［入力配線に関する処理］
全ての計算装置
【０２３７】
【数７９】

$$\{u_\alpha\}$$

【０２３８】
は、全てのk=m+1,...,m+n、全ての
【０２３９】
【数８０】

$$\varepsilon \in [0,1]$$

【０２４０】
に関して
【０２４１】
【数８１】

$$r^{\sim(\alpha)}\varepsilon_k \in_R Z/qZ$$

【０２４２】
を一様無作為に生成し、
全てのk=m+1,...,m+n、全ての

【０２４３】
【数８２】

$$b, \varepsilon \in \{0,1\}$$

【０２４４】
に関して楕円ElGamal暗号方式を用いて、入力の暗号文
【０２４５】
【数８３】

$$(C(\alpha)b\varepsilon_{[k]}, D(\alpha)b\varepsilon_{[k]}) = ([r\tilde{}(\alpha)\varepsilon_{[k]}]G, X(\alpha)\varepsilon_{[k]} + [r\tilde{}(\alpha)\varepsilon_{[k]}](Y\tilde{}b_{[k]} + Z))$$

【０２４６】
を生成し（図８の120）、これらを公開する（図８の121）。
併せて、それぞれのkに関して、全ての
【０２４７】
【数８４】

$$b, \in \{0,1\}$$

【０２４８】
に関して、楕円ElGamal暗号文
【０２４９】
【数８５】

$$(C(\alpha)b0_{[k]}, D(\alpha)b0_{[k]})$$

【０２５０】
の復号結果が同じになること、それぞれのkに関して、全ての
【０２５１】
【数８６】

$$b \in \{0,1\}$$

【０２５２】
に関して、楕円ElGamal暗号文
【０２５３】
【数８７】

$$(C(\alpha)b1_{[k]}, D(\alpha)b1_{[k]})$$

【０２５４】
の復号結果が同じになることの証明を、別記述Dの方法で、入力の暗号文の正当性証明として生成し（図８の122）、公開する（図８の123）。
【０２５５】
全ての計算装置
【０２５６】

【数８８】

$$\{u_{\alpha}\}$$

【０２５７】
は各自、全てのk=m+1,...,m+n、全ての
【０２５８】
【数８９】

$$b,\xi \in \{0,1\}$$

【０２５９】
に関して、入力の暗号文識別データの暗号文
【０２６０】
【数９０】

$$(A^{(0)b}{}_{[k]\xi}, B^{(0)b}{}_{[k]\xi}) = (O,[\varepsilon]G)\ \{(C^{(0)\alpha b}{}_{[k]\xi}, D^{(0)\alpha b}{}_{[k]\xi})\}_{\alpha=1,\ldots,\lambda} = \{(C^{(\alpha)b\varepsilon}{}_{[k]}, D^{(\alpha)b\varepsilon}{}_{[k]})\}_{\alpha=1,\ldots,\lambda}$$

【０２６１】
を生成する（図８の124）。但し
【０２６２】
【数９１】

$$\varepsilon = b \square \xi$$

【０２６３】
。
[出力配線に関する処理]
全ての計算装置
【０２６４】
【数９２】

$$\{u_{\alpha}\}$$

【０２６５】
は各自、全ての配線k=1,...,l、全ての
【０２６６】
【数９３】

$$b,\varepsilon \in \{0,1\}$$

【０２６７】
に関して、出力の暗号文
【０２６８】
【数９４】

$$(A^{\dagger(0)b}{}_{[k]\xi}, B^{\dagger(0)b}{}_{[k]\xi}), \&=\& (O,[\varepsilon]G)$$

【０２６９】
を生成する（図８の125）。但し
【０２７０】
【数９５】

$$\varepsilon = b \square \xi$$

【０２７１】
。
【０２７２】
［逐次置換再暗号処理201 --- ゲート暗号文の置換と再暗号］
次に、図６に示されるように、逐次置換再暗号処理２０１が行なわれる。この逐次置換再暗号処理２０１について、処理を詳細に示す図９および図１２を参照して説明する。
【０２７３】
$\alpha=1,\ldots,\lambda$に関して順番に、計算装置u_αは以下の処理（図１２の304）を行う（図９の126）。この処理で各計算装置は、最初に公開情報取得手段を用いて必要なデータを取得し（図１２の310）、次に生成したデータを情報公開手段を用いて公開する（図１２の311）。λ個の計算装置には順番が定められており、それぞれの計算装置がデータを取得するには、この計算機よりも順番が前の計算機全てがデータの公開を終了しておかねばならない。
【０２７４】
［暗号文取得処理］
【０２７５】
【数９６】

$$u_\alpha$$

【０２７６】
は、$k=1,\ldots,m$、全ての$\beta=1,\ldots,\lambda$、全ての
【０２７７】
【数９７】

$$b,c,\mu,\nu,\xi \in \{0,1\}$$

【０２７８】
に関する
【０２７９】
【数９８】

$$A^{(\alpha-1)bc}{}_{[k]\mu,\nu,\xi},\ B^{(\alpha-1)bc}{}_{[k]\mu,\nu,\xi},\ C^{(\alpha-1)\beta bc}{}_{[k]\mu,\nu,\xi},\ D^{(\alpha-1)\beta bc}{}_{[k]\mu,\nu,\xi},$$

【０２８０】
全ての$k=m+1,\ldots,m+n$、全ての$\beta=1,\ldots,\lambda$、全ての
【０２８１】

【数９９】

$$b,\xi \in \{0,1\}$$

【０２８２】
に関する
【０２８３】
【数１００】

$$A^{(\alpha-1)b_{[k]\xi}}, B^{(\alpha-1)b_{[k]\xi}}, C^{(\alpha-1)\beta b_{[k]\xi}}, D^{(\alpha-1)\beta b_{[k]\xi}},$$

【０２８４】
全てのk=1,...,l、全ての
【０２８５】
【数１０１】

$$b,\xi \in \{0,1\}$$

【０２８６】
、に関する
【０２８７】
【数１０２】

$$A^{\dagger(\alpha-1)b_{[k]\xi}}, B^{\dagger(\alpha-1)b_{[k]\xi}}$$

【０２８８】
を取得する（図９の151）。
【０２８９】
[配線の信号値と置換生成]
【０２９０】
【数１０３】

$$u_{\alpha}$$

【０２９１】
は、各配線の信号値の置換
【０２９２】
【数１０４】

$$\{\pi(k) \in_R \{0,1\}\}_{k=1,...,m+n},$$

【０２９３】
を一様無作為に生成する（図９の127）。
【０２９４】
[再暗号化の乱数生成]
【０２９５】

【数１０５】

$$u_{\alpha}$$

【０２９６】
は、ゲートの秘密鍵の再暗号化に使う乱数
【０２９７】
【数１０６】

$$\{s^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi\}_{k=1,\ldots,m;b,c,\mu,\nu,\xi\in R\{0,1\}}$$

$$\{t^{(\alpha)\beta bc}{}_{[k]}\mu,\nu,\xi\}_{k=1,\ldots,m;\beta=1,\ldots,\beta;b,c,\mu,\nu,\xi\in R\{0,1\}}$$

$$\{s^{(\alpha)b}{}_{[k]}\xi\}_{k=m+1,\ldots,m+n;b,\xi\in R\{0,1\}}$$

$$\{t^{(\alpha)\beta b}{}_{[k]}\xi\}_{k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda;b,\xi\in R\{0,1\}}$$

$$\{s^{\dagger b}{}_{[k]}\xi\}_{k=1,\ldots,l;b,\xi\in R\{0,1\}}$$

【０２９８】
を一様無作為に生成する（図９の128）。
【０２９９】
［ゲートの秘密鍵の暗号文の置換と再暗号化］
全てのk=1,...,m、全ての$\beta=1,\ldots,\lambda$、全ての
【０３００】
【数１０７】

$$b,c,\mu,\nu,\xi\in\{0,1\}$$

【０３０１】
に関して、
【０３０２】
【数１０８】

$$A^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi = A^{(\alpha-1)bc}{}_{[k]}\mu\square\pi(i),\nu\square\pi(j),\xi\square\pi(k)^{+}\,[s^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi]G$$

$$B^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi = B^{(\alpha-1)bc}{}_{[k]}\mu\square\pi(i),\nu\square\pi(j),\xi\square\pi(k)^{+}$$
$$[s^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

$$C^{(\alpha)\beta bc}{}_{[k]}\mu,\nu,\xi = C^{(\alpha-1)\beta bc}{}_{[k]}\mu\square\pi(i),\nu\square\pi(j),\xi\square\pi(k)^{+}[t^{(\alpha)\beta bc}{}_{[k]}\mu,\nu,\xi]G$$

$$D^{(\alpha)\beta bc}{}_{[k]}\mu,\nu,\xi = D^{(\alpha-1)\beta bc}{}_{[k]}\mu\square\pi(i),\nu\square\pi(j),\xi\square\pi(k)$$
$$+[t^{(\alpha)\beta bc}{}_{[k]}\mu,\nu,\xi](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

【０３０３】

と、ゲート秘密鍵を置換し再暗号化したデータを生成し（図９の129）、
［入力の暗号文の置換と再暗号化］
全てのk=m+1,...,m+n、全てのβ=1,...,λ、全ての
【０３０４】
【数１０９】

$$b,\xi \in \{0,1\}$$

【０３０５】
に関して、
【０３０６】
【数１１０】

$$A^{(\alpha)b}{}_{[k]\xi} = A^{(\alpha-1)b}{}_{[k]\xi} \square \pi(k) + [s^{(\alpha)b}{}_{[k]\xi}]G$$

$$B^{(\alpha)b}{}_{[k]\xi} = B^{(\alpha-1)b}{}_{[k]\xi} \square \pi(k) + [s^{(\alpha)b}{}_{[k]\xi}](Y^{\sim b}{}_{[k]} + Z)$$

$$C^{(\alpha)\beta b}{}_{[k]\xi} = C^{(\alpha-1)\beta b,sub>}{}_{[k]\xi} \square \pi(k) + [t^{(\alpha)b}{}_{[k]\xi}]G$$

$$D^{(\alpha)\beta b}{}_{[k]\xi} = D^{(\alpha-1)\beta b}{}_{[k]\xi} \square \pi(k) + [t^{(\alpha)b}{}_{[k]\xi}](Y^{\sim b}{}_{[k]} + Z)$$

【０３０７】
と、入力の暗号文を置換し再暗号化したデータを生成し（図９の130）、
［出力の暗号文の置換と再暗号化］
全てのk=1,...,l、全ての
【０３０８】
【数１１１】

$$b,\xi \in \{0,1\}$$

【０３０９】
、に関して，
【０３１０】
【数１１２】

$$A^{\dagger(\alpha)b}{}_{[k]\xi} = A^{\dagger(\alpha-1)b}{}_{[k]\xi} \square \pi(k) + [s^{\dagger b}{}_{[k]\xi}]G$$

$$B^{\dagger(\alpha)b}{}_{[k]\xi} = B^{\dagger(\alpha-1)b}{}_{[k]\xi} \square \pi(k) + [s^{\dagger b}{}_{[k]\xi}](Y^{b}{}_{[k]} + Z)$$

【０３１１】
と、出力の暗号文を置換し再暗号化したデータを生成し（図９の131）、
［置換と再暗号化の正当性証明］
全てのk=1,...,m、全てのβ=1,...,λ、全ての
【０３１２】

【数１１３】

$$b,c,\mu,\nu,\xi \in \{0,1\}$$

【０３１３】
に関する
【０３１４】
【数１１４】

$$\{A(\alpha)bc_{[k]\mu,\nu,\xi}, B(\alpha)bc_{[k]\mu,\nu,\xi}, C(\alpha)\beta bc_{[k]\mu,\nu,\xi}, D(\alpha)\beta bc_{[k]\mu,\nu,\xi}\}$$

【０３１５】
及び、
全てのk=m+1,...,m+n、全てのβ=1,...,λ、全ての
【０３１６】
【数１１５】

$$b,\xi \in \{0,1\}$$

【０３１７】
に関する
【０３１８】
【数１１６】

$$\{A(\alpha)b_{[k]\xi}, B(\alpha)b_{[k]\xi}, C(\alpha)\beta b_{[k]\xi}, D(\alpha)\beta b_{[k]\xi}\}$$

【０３１９】
及び
全てのk=1,...,l、全ての
【０３２０】
【数１１７】

$$b,\xi \in \{0,1\} \text{に関する} \{A^{\dagger}(\alpha)b_{[k]\xi}, B^{\dagger}(\alpha)b_{[k]\xi}\}$$

【０３２１】
を
【０３２２】
【数１１８】

$$u_{\alpha+1}$$

【０３２３】
に送信する。
【０３２４】
併せて上記処理を正当に行ったことの証明を、別記述Eの方法に従って、ゲートの秘密鍵の暗号文と入力の暗号文と出力の暗号文との置換と再暗号化の正当性証明として生成し公開する（図９の132）。
【０３２５】
[結果出力処理202,305]
次に、図６に示されるように、結果出力処理２０２が行なわれる。この結果出力処理２

０２について、処理を詳細に示す図１０ないし図１２を参照して説明する。

【０３２６】

結果出力処理２０２では情報公開手段と公開情報取得手段を使って、データの公開と取得の両方を行う（図１２の312）。最後に、各自回路の出力（図１２の306）を出力する（図１２の313）。

【０３２７】

[ゲート暗号文の部分復号]

全ての計算装置

【０３２８】

【数１１９】

$$\{u_\alpha\}_{\alpha=1,\ldots,\lambda}$$

【０３２９】

は、全ての

【０３３０】

【数１２０】

$$k=1,\ldots,m,\ b,c \in \{0,1\},\ \beta=1,\ldots,\lambda$$

【０３３１】

に関して、

【０３３２】

【数１２１】

$$A^{\sharp(\lambda)\alpha}bc_{[k]000}=[z(\alpha)]A(\lambda)bc_{[k]000}$$

$$C^{\sharp(\lambda)\alpha\beta}bc_{[k]000}=[z(\alpha)]C(\lambda)\beta bc_{[k]000}$$

【０３３３】

と、ゲート秘密鍵を部分復号し、結果を公開し（図１０の134）、全ての計算装置

【０３３４】

【数１２２】

$$\{u_\alpha\}_{\alpha=1,\ldots,\lambda}$$

【０３３５】

は、全ての

【０３３６】

【数１２３】

$$k=m+1,\ldots,m+n,\ b \in \{0,1\},\ \beta=1,\ldots,\lambda$$

【０３３７】

に関して

【０３３８】

【数１２４】

$$A^{\#(\lambda)\alpha}b_{[k]0}=[z(\alpha)]A^{(\lambda)}b_{[k]0}$$

$$C^{\#(\lambda)\alpha\beta}b_{[k]0}=[z(\alpha)]C^{(\lambda)\beta}b_{[k]0}$$

【０３３９】
と、入力の暗号文を部分復号し、結果を公開し（図１０の135）、
全ての計算装置
【０３４０】
【数１２５】

$$\{u_\alpha\}_{\alpha=1,\ldots,\lambda}\ \text{は},\ k=1,\ldots,l,\ b\in\{0,1\}$$

【０３４１】
に関して
【０３４２】
【数１２６】

$$A^{\dagger\#(\lambda)\alpha}b_{[k]0}=[z(\alpha)]A^{\dagger(\lambda)}b_{[k]0}$$

【０３４３】
と、出力の暗号文を部分復号し、結果を公開する（図１０の136）。
【０３４４】
併せて上記処理を正当に行ったことの証明を別記述Fの方法に従って、ゲート秘密鍵と入力の暗号文と出力の暗号文との部分復号の正当性証明として生成し公開する（図１０の137）。
【０３４５】
［ゲート暗号文の生成］
全ての計算装置は、さらに全てのk=1,...,m、全ての$\alpha=1,\ldots,\lambda$、全ての
【０３４６】
【数１２７】

$$b,c,\in\{0,1\}$$

【０３４７】
に関して、
【０３４８】
【数１２８】

$$A^{bc}{}_{[k]}=A^{(\lambda)bc}{}_{[k]000}$$

$$B^{bc}{}_{[k]}=B^{(\lambda)bc}{}_{[k]000}-\Sigma_{\alpha=1}{}^{\lambda}\ A^{\#(\lambda)\alpha bc}{}_{[k]000}$$

$$C^{\alpha bc}{}_{[k]}=C^{(\lambda)\alpha bc}{}_{[k]000}$$

$$D^{\alpha bc}{}_{[k]}=D^{(\lambda)\alpha bc}{}_{[k]000}-\Sigma_{\alpha=1}{}^{\lambda}\ C^{\#(\lambda)\alpha\beta bc}{}_{[k]000}$$

【０３４９】

を、
全てのk=m+1,...,m+n、全てのα=1,...,λ、全ての
【０３５０】
【数１２９】

$$b_{\cdot} \in \{0,1\}$$

【０３５１】
に関して、
【０３５２】
【数１３０】

$$A^{b}{}_{[k]} = A^{(\lambda)b}{}_{[k]0}$$

$$B^{b}{}_{[k]} = B^{(\lambda)b}{}_{[k]0} - \Sigma_{\alpha=1}^{\lambda} A^{\sharp(\lambda)\alpha b}{}_{[k]0}$$

$$C^{\alpha b}{}_{[k]} = C^{(\lambda)\alpha b}{}_{[k]0}$$

$$D^{\alpha b}{}_{[k]} = D^{(\lambda)\alpha b}{}_{[k]0} - \Sigma_{\alpha=1}^{\lambda} C^{\sharp(\lambda)\alpha\beta b}{}_{[k]0}$$

【０３５３】
を、全ての k=1,...,l、全ての
【０３５４】
【数１３１】

$$b \in \{0,1\}$$

【０３５５】
に関して、
【０３５６】
【数１３２】

$$A^{\dagger b}{}_{[k]} = A^{\dagger(\lambda)b}{}_{[k]0}$$

$$B^{\dagger b}{}_{[k]} = B^{\dagger(\lambda)b}{}_{[k]0} - A^{\dagger\sharp(\lambda)\alpha b}{}_{[k]0}$$

【０３５７】
をゲート暗号文として生成する（図１０の138）。
【０３５８】
[入力の復号]
各計算装置
【０３５９】
【数１３３】

$$u^{(\alpha)} \text{は, 全ての } k=m+1+\Sigma_{\gamma=1}^{\alpha-1} I_{\gamma},\ldots,m+\Sigma_{\gamma=1}^{\alpha} I_{\gamma}$$

【０３６０】

、全ての$\beta=1,\ldots,\lambda$に関して、b「k」を開示することなく

【０３６１】

【数１３４】

$$G^{b}{}_{[k]}=B^{b\lceil k\rfloor}{}_{[k]}-[x^{\sim b\lceil k\rfloor}{}_{[k]}]A^{b\lceil k\rfloor}{}_{[k]}$$

$$X^{b}(\beta)_{[k]}=D^{\beta\, b\lceil k\rfloor}{}_{[k]}-[x^{\sim b\lceil k\rfloor}{}_{[k]}]C^{\beta\, b\lceil k\rfloor}{}_{[k]}$$

$$x^{b}(\beta)_{[k]}=\phi(X^{b}(\beta)_{[k]})$$

【０３６２】

を生成し、公開する（図１０の139）。この公開したデータは入力の暗号文を復号したデータと呼ぶ。

【０３６３】

全ての計算装置

【０３６４】

【数１３５】

$$u_{\alpha}$$

【０３６５】

は、全てのk=m+1,...,m+n、全ての$\beta=1,\ldots,\lambda$に関して、

【０３６６】

【数１３６】

$$Y(\beta)\varepsilon\lceil k\rfloor_{[k]} := [x^{b}(\beta)_{[k]}]G$$

【０３６７】

を確認することで、入力の暗号文の復号の正当性を確認する（図１０の140）。但し、もし

【０３６８】

【数１３７】

$$G^{b}{}_{[k]}=0 \text{ ならば } \varepsilon_{k}=0,\ G^{b}{}_{[k]}=G \text{ ならば } \varepsilon_{k}=1$$

【０３６９】

とする。

【０３７０】

[回路の評価]

全ての計算装置

【０３７１】

【数１３８】

$$u_{\alpha}$$

【０３７２】

はそれぞれ、全てのゲート$G_{k\,k=1,\ldots,m}$に関して適切な順番に、それらの入力から出力を

以下のように求めていく（図１０の141）。これが回路の評価の処理である。但しゲートG_kにはゲートG_iとゲートG_jの出力が入力されるとする。

【０３７３】

全ての$\beta=1,\ldots,\lambda$に関して，

【０３７４】

【数１３９】

$$G^{b}{}_{[k]}=B^{b\lceil i\rfloor b\lceil j\rfloor}{}_{[k]}-[\Sigma_{\gamma=1}\lambda(x(\gamma)b\lceil i\rfloor_{[k]}+x(\gamma)b\lceil j\rfloor_{[k]})]\,A^{b\lceil i\rfloor b\lceil j\rfloor}{}_{[k]}$$

$$X^{b}(\beta)_{[k]}=D^{\beta\ b\lceil i\rfloor\ b\lceil j\rfloor}{}_{[k]}-[\Sigma_{\gamma=1}\lambda(x(\gamma)b\lceil i\rfloor_{[k]}+x(\gamma)b\lceil j\rfloor_{[k]})]\,C^{\beta\ b\lceil i\rfloor\ b\lceil j\rfloor}{}_{[k]}$$

$$x^{b}(\beta)_{[k]}=\phi(X^{b}(\beta)_{[k]})$$

【０３７５】

を求め（図１０の142）、

$\beta=1,\ldots,\lambda$に関して，

【０３７６】

【数１４０】

$$Y(\beta)\varepsilon\lceil k\rfloor_{[k]}\quad=\quad[x^{b}(\beta)_{[k]}]G$$

【０３７７】

を確認する（図１０の143）。但し、もし

【０３７８】

【数１４１】

$$G^{b}{}_{[k]}=O\ \text{なら}\ \varepsilon_k=0,\ G^{b}{}_{[k]}=G\ \text{なら}\ \varepsilon_k=1$$

【０３７９】

とする。上記処理を行ったkに関して、

【０３８０】

【数１４２】

$$b\lceil k\rfloor=\varepsilon_k$$

【０３８１】

とする。

【０３８２】

[出力の評価]

ここまでの処理で公開した証明を検証者は検証する（図１０の144）。検証者が全ての証明文を受理したならば、すなわち不正が発見されなかったならば、以下の出力の復号と公開の処理を行う。

【０３８３】

全ての計算装置

【０３８４】

【数１４３】

$$u_{\alpha}$$

【０３８５】
はそれぞれ、全てのk=1,...,lに関して,
【０３８６】
【数１４４】

$$G^{\dagger}_{[k]}=B^{\dagger b\lceil k\rfloor}_{[k]}-[\Sigma_{\gamma=1}\lambda(x(\gamma)b^{\lceil k\rfloor}_{[k]}]A^{\dagger b\lceil k\rfloor}_{[k]}$$

【０３８７】
を求める（図１０の145）。
【０３８８】
全ての
【０３８９】
【数１４５】

$$[u_{\alpha}]_{\alpha=1,\ldots,\lambda}$$

【０３９０】
はそれぞれ、全てのk=1,...,lに関して,
【０３９１】
【数１４６】

$$A^{\dagger\sharp}_{[k]}=[z(\alpha)]A^{\dagger b\lceil k\rfloor}_{[k]}$$

【０３９２】
を生成して（図１０の146）公開する（図１０の147）。
【０３９３】
併せてこの計算の正当性の証明を、別記述Gの方法に従って、出力の復号の正当性の証明生成と（図１０の148）して公開する（図１０の149）。
【０３９４】
それぞれの
【０３９５】
【数１４７】

$$u_{\alpha}$$

【０３９６】
は、各自
【０３９７】
【数１４８】

$$G^{\flat}_{[k]}=G^{\dagger}_{[k]}-\Sigma_{\gamma=1}\lambda\ A^{\dagger\sharp}_{[k]}$$

【０３９８】
から回路の出力（図１１の306）を求める（図１０の150）。
【０３９９】
k=1,...,l に関して、

【０４００】
【数１４９】

$$G\sharp_{[k]}=O$$

【０４０１】
ならばb「k」=0であり、
【０４０２】
【数１５０】

$$G\sharp_{[k]}=G$$

【０４０３】
ならばb「k」=1である。
【０４０４】
[別記述処理]
[別記述A]
証明者(計算者)
【０４０５】
【数１５１】

$$u_{\alpha}$$

【０４０６】
は、全てのk=1,...,m+n、全ての
【０４０７】
【数１５２】

$$b\in\{0,1\}$$

【０４０８】
に関して,
【０４０９】
【数１５３】

$$x'(\alpha)b_{[k]} \in_R Z/qZ$$

$$z'(\alpha) \in_R Z/qZ$$

【０４１０】
を一様無作為に生成し,
【０４１１】
【数１５４】

$$Y'(\alpha)b_{[k]} = [x'(\alpha)b_{[k]}]G$$

$$Z'(\alpha) = [z'(\alpha)]G$$

【０４１２】
を生成する。さらに，
【０４１３】
【数１５５】

$$\theta = \mathrm{Hash}(E,G,\{Y'^{(\alpha)}{}_{b_{[k]}}\}_{k=1,\ldots,m+n;b=0,1}, Z^{(\alpha)}, \{Y''^{(\alpha)}{}_{b_{[k]}}\}_{k=1,\ldots,m+n;b=0,1}, Z'^{(\alpha)}) \bmod q$$

【０４１４】
を生成し、全てのk=1,...,m+n、全ての
【０４１５】
【数１５６】

$$b \in \{0,1\}$$

【０４１６】
に関して、
【０４１７】
【数１５７】

$$x''^{(\alpha)}{}_{b_{[k]}} = \theta\ x^{(\alpha)}{}_{b_{[k]}} + x'^{(\alpha)}{}_{b_{[k]}} \bmod q$$

$$z''^{(\alpha)} = \theta\ z^{(\alpha)} + z'^{(\alpha)} \bmod q$$

【０４１８】
を生成する。証明者は、全てのk=1,...,m+n、全ての
【０４１９】
【数１５８】

$$b \in \{0,1\}$$

【０４２０】
に関する
【０４２１】
【数１５９】

$$Y'^{(\alpha)}{}_{b_{[k]}}, Z'^{(\alpha)}, x''^{(\alpha)}{}_{b_{[k]}}, z''^{(\alpha)}$$

【０４２２】
を証明とする。上記証明の検証方法は以下の通り。
検証者は、
【０４２３】
【数１６０】

$$\theta = \mathrm{Hash}(E,G,\{Y^{(\alpha)}{}_{b_{[k]}}\}_{k=1,\ldots,m+n;b=0,1}, Z^{(\alpha)}, \{Y'^{(\alpha)}{}_{b_{[k]}}\}_{k=1,\ldots,m+n;b=0,1}, Z'^{(\alpha)}) \bmod q$$

【０４２４】
を計算して、
【０４２５】

【数１６１】

$$[x''(\alpha)b_{[k]}]G = [\theta]Y(\alpha)b_{[k]} + Y'(\alpha)b_{[k]}$$

$$[z''(\alpha)]G = \theta\ Z(\alpha) + Z'(\alpha)$$

【０４２６】
を確認する。
【０４２７】
[別記述B]
各証明者(計算者)
【０４２８】
【数１６２】

$$u(\alpha)$$

【０４２９】
は、全ての
【０４３０】
【数１６３】

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1}I_{\beta},\ldots,m+\Sigma_{\beta=1}^{\alpha}I_{\beta}$$

【０４３１】
に関して、選択した
【０４３２】
【数１６４】

$$b\lceil k\rfloor \in \{0,1\}$$

【０４３３】
に対して，
【０４３４】
【数１６５】

$$x^{\sim}{}'b\lceil k\rfloor_{[k]} \in_R Z/qZ$$

【０４３５】
を一様無作為に生成し、
【０４３６】
【数１６６】

$$Y^{\sim}{}'b\lceil k\rfloor_{[k]} = [x^{\sim}{}'b\lceil k\rfloor_{[k]}]G$$

【０４３７】
を生成する。
さらに、
【０４３８】

【数１６７】

$$\theta^{b\lceil k\rfloor\square 1}{}_{[k]} \in_R Z/qZ$$

$$\tilde{x}''^{b\lceil k\rfloor\square 1}{}_{[k]} \in_R Z/qZ$$

【０４３９】
を無作為に生成し，
【０４４０】
【数１６８】

$$\tilde{Y}''^{b\lceil k\rfloor\square 1}{}_{[k]} = [\tilde{x}''^{b\lceil k\rfloor\square 1}{}_{[k]}]G - [\theta^{b\lceil k\rfloor\square 1}{}_{[k]}]\,\tilde{Y}^{b\lceil k\rfloor\square 1}{}_{[k]}$$

【０４４１】
を生成する。
【０４４２】
【数１６９】

$$^{u}\alpha$$

【０４４３】
は、全ての
【０４４４】
【数１７０】

$$k=m+1+\Sigma_{\beta=1}{}^{\alpha-1}I_{\beta},\ldots,m+\Sigma_{\beta=1}{}^{\alpha}I_{\beta}$$

【０４４５】
に関して、
【０４４６】
【数１７１】

$$\theta_{[k]} = \mathrm{Hash}(E,G,\{\tilde{Y}^{b}{}_{[k]},\tilde{Y}^{b}{}_{[k]}\}_{b=0,1}) \bmod q$$

$$\theta^{b\lceil k\rfloor}{}_{[k]} = \theta_{[k]} - \theta^{b\lceil k\rfloor\square 1}{}_{[k]} \bmod q$$

【０４４７】
を生成する。
さらに、
【０４４８】
【数１７２】

$$\tilde{x}''^{b\lceil k\rfloor}{}_{[k]} = \theta^{b\lceil k\rfloor}{}_{[k]}\,\tilde{x}^{b\lceil k\rfloor}{}_{[k]} + \tilde{x}''^{b\lceil k\rfloor}{}_{[k]} \bmod q$$

【０４４９】
を生成する。
【０４５０】
証明者

【０４５１】
【数１７３】

$$u_{\alpha}$$

【０４５２】
は、全ての
【０４５３】
【数１７４】

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1} I_{\beta},\ldots,m+\Sigma_{\beta=1}^{\alpha} I_{\beta},\ b=0,1$$

【０４５４】
に関する
【０４５５】
【数１７５】

$$Y^{\sim,b}_{[k]},\ \theta^{0}_{[k]},\ x^{\sim,b}_{[k]}$$

【０４５６】
を証明とする。
【０４５７】
上記証明の検証方法は以下の通り。
【０４５８】
検証者は、全ての
【０４５９】
【数１７６】

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1} I_{\beta},\ldots,m+\Sigma_{\beta=1}^{\alpha} I_{\beta},\ b=0,1$$

【０４６０】
に関して、
【０４６１】
【数１７７】

$$\theta_{[k]} = \mathrm{Hash}(E,G,[Y^{\sim b}_{[k]}, Y^{\sim,b}_{[k]}]_{b=0,1}) \bmod q$$

$$\theta^{1}_{[k]} = \theta_{[k]} - \theta^{0}_{[k]} \bmod q$$

【０４６２】
を生成し、全ての
【０４６３】
【数１７８】

$$k=m+1+\Sigma_{\beta=1}^{\alpha-1} I_{\beta},\ldots,m+\Sigma_{\beta=1}^{\alpha} I_{\beta},\ b=0,1$$

【０４６４】
に関して、
【０４６５】

【数１７９】

$$[x^{\sim,,b}{}_{[k]}]G = [\theta^{b}{}_{[k]}]\, Y^{\sim b}{}_{[k]} + Y^{\sim,b}{}_{[k]}$$

$$Y^{\sim 0}{}_{[k]} + Y^{\sim 1}{}_{[k]} = H$$

【０４６６】
が成り立つことを確認する。
【０４６７】
［別記述C］
証明者(計算者)
【０４６８】
【数１８０】

$$u_{\alpha}$$

【０４６９】
は、全てのk=1,...,m、全てのε=0,1に関して、
【０４７０】
【数１８１】

$$r'(\alpha)\varepsilon 0_{[k]} \in Z/qZ$$

【０４７１】
を一様無作為に生成して、
【０４７２】
【数１８２】

$$F(\alpha)\varepsilon 0_{[k]} = [r'(\alpha)\varepsilon 0_{[k]}]G$$

$$F(\alpha)\varepsilon 1_{[k]} = [r'(\alpha)\varepsilon 1_{[k]}]\,(Y^{1}{}_{[i]} - Y^{0}{}_{[i]})$$

$$F(\alpha)\varepsilon 2_{[k]} = [r'(\alpha)\varepsilon 2_{[k]}]\,(Y^{1}{}_{[j]} - Y^{0}{}_{[j]})$$

【０４７３】
を生成する。
【０４７４】
さらに、
【０４７５】
【数１８３】

$$\theta(\alpha)_{[k]'} = \mathrm{Hash}\,(E,G,\{C^{(\alpha)bc}{}_{\varepsilon\,[k]}, D^{(\alpha)bc}{}_{\varepsilon\,[k]}\}_{k=1,...,m;b,c,\varepsilon=0,1}, \{F(\alpha)\varepsilon 0_{[k]}, F(\alpha)\varepsilon 1_{[k]}, F(\alpha)\varepsilon 2_{[k]},\}_{k=1,...,m;\varepsilon=0,1})$$

【０４７６】
を生成する。

【０４７７】
次に、
【０４７８】
【数１８４】

$$r''(\alpha)\varepsilon_{[k]} = \theta(\alpha)_{[k]}\, r(\alpha)\varepsilon_{[k]} + r'(\alpha)\varepsilon_{[k]} \bmod q$$

【０４７９】
を生成する。
証明者は、k=1,...,m及びε=0,1に関する
【０４８０】
【数１８５】

$$F(\alpha)\varepsilon 0_{[k]},\ F(\alpha)\varepsilon 1_{[k]},\ F(\alpha)\varepsilon 2_{[k]},\ r''(\alpha)\varepsilon_{[k]}$$

【０４８１】
を証明とする。
【０４８２】
上記証明の検証方法は以下の通り。
【０４８３】
検証者は、最初にそれぞれのε=0,1、及びk=1,...,mに関して、全てのb,c=0,1に対する
【０４８４】
【数１８６】

$$C(\alpha)bc\ \varepsilon_{[k]}$$

【０４８５】
が全て同じ値であることを確認する。
【０４８６】
次に、
【０４８７】
【数１８７】

$$\theta(\alpha)_{[k]}, = \mathrm{Hash}\,(E,G,\{C(\alpha)bc\ \varepsilon_{[k]}, D(\alpha)bc\ \varepsilon_{[k]}\}_{k=1,...,m;b,c,\varepsilon=0,1}, \{F(\alpha)\varepsilon 0_{[k]}, F(\alpha)\varepsilon 1_{[k]}, F(\alpha)\varepsilon 2_{[k]},\}_{k=1,...,m;\varepsilon=0,1})$$

【０４８８】
を生成する。次に、すべてのk=1,...,m及びε=0,1に関して
【０４８９】

【数１８８】

$$[r''(\alpha)\varepsilon_{[k]}]G = [\theta(\alpha)_{[k]}]\, C(\alpha)00\,\varepsilon_{[k]} + F(\alpha)\varepsilon 0_{[k]}$$

$$[r''(\alpha)\,\varepsilon_{[k]}]\,(Y^1_{[j]} - Y^0_{[j]}) = [\theta(\alpha)_{[k]}]\,(D(\alpha)01\,\varepsilon_{[k]} - D(\alpha)00\,\varepsilon_{[k]}) + F(\alpha)\varepsilon 2_{[k]}$$

$$[r''(\alpha)\,\varepsilon_{[k]}]\,(Y^1_{[i]} - Y^0_{[i]}) = [\theta(\alpha)_{[k]}]\,(D(\alpha)10\,\varepsilon_{[k]} - D(\alpha)00\,\varepsilon_{[k]}) + F(\alpha)\varepsilon 1_{[k]}$$

$$(D(\alpha)11\,\varepsilon_{[k]} - D(\alpha)10\,\varepsilon_{[k]}) = (D(\alpha)01\,\varepsilon_{[k]} - D(\alpha)00\,\varepsilon_{[k]})$$

【０４９０】
が成り立つことを確認する。
【０４９１】
[別記述D]
証明者(計算者)u_αは、全てのk=m+1,...,m+n、全てのb, ε=0,1に関して、
【０４９２】
【数１８９】

$$r'(\alpha)b_{[k]} \in Z/qZ$$

【０４９３】
を一様無作為に生成して,
【０４９４】
【数１９０】

$$F(\alpha)\varepsilon 0_{[k]} = [r\tilde{}''(\alpha)\varepsilon_{[k]}]G$$

$$F(\alpha)\varepsilon 1_{[k]} = [r\tilde{}''(\alpha)\varepsilon_{[k]}]\,(Y\tilde{}^1_{[k]} - Y\tilde{}^0_{[k]})$$

【０４９５】
を生成する。
さらに、全てのk=m+1,...,m+nに関して
【０４９６】
【数１９１】

$$\theta(\alpha)_{[k]'} = \mathrm{Hash}\,(E,G,\{C(\alpha)b\,\varepsilon_{[k]}, D(\alpha)b\,\varepsilon_{[k]}, F(\alpha)b\,\varepsilon_{[k]}\}_{k=m+1,\ldots,m+n;b,\varepsilon=0,1})$$

【０４９７】
を生成する。
【０４９８】
次に、全てのk=m+1,...,m+n、全てのb, ε=0,1に関して,
【０４９９】
【数１９２】

$$r\tilde{}''(\alpha)\varepsilon_{[k]} = \theta(\alpha)_{[k]}\, r\tilde{}(\alpha)\varepsilon_{[k]} + r\tilde{}''(\alpha)\varepsilon_{[k]} \bmod q$$

【０５００】
を生成する。
証明者は、k=m+1,...,m+n及びε=0,1に関する

【０５０１】
【数１９３】

$$F(\alpha)\varepsilon 0_{[k]},\ F(\alpha)\varepsilon 1_{[k]},\ r^{\sim\prime\prime}(\alpha)\varepsilon_{[k]}$$

【０５０２】
を証明とする。
【０５０３】
上記証明の検証方法は以下の通り。検証者は、最初にそれぞれの$\varepsilon=0,1$、及び$k=1,\ldots,m$に関して、全ての$b=0,1$に対する
【０５０４】
【数１９４】

$$C(\alpha)b\varepsilon_{[k]}$$

【０５０５】
が全て同じ値であることを確認する。
【０５０６】
次に、
【０５０７】
【数１９５】

$$\theta(\alpha)_{[k]},=\mathrm{Hash}\ (E,G,\{\ C(\alpha)b\varepsilon_{[k]},\ D(\alpha)b\varepsilon_{[k]},\ F(\alpha)b\varepsilon_{[k]}\ \}_{k=m+1,\ldots,m+n;b,\varepsilon=0,1}\ )$$

【０５０８】
を生成する。
【０５０９】
次に、すべての$k=m+1,\ldots,m+n$及び$\varepsilon=0,1$に関して
【０５１０】
【数１９６】

$$[r^{\sim\prime\prime}(\alpha)\varepsilon_{[k]}]G=[\theta(\alpha)_{[k]}]\ C(\alpha)0\varepsilon_{[k]}+F(\alpha)\varepsilon 0_{[k]}$$

$$[r^{\sim\prime\prime}(\alpha)\ \varepsilon_{[k]}]\ (Y^{\sim}1_{[j]}-Y^{\sim}0_{[j]})=[\theta(\alpha)_{[k]}]\ (D(\alpha)1\ \varepsilon_{[k]}-D(\alpha)0\varepsilon_{[k]})+F(\alpha)\varepsilon 1_{[k]}$$

【０５１１】
が成り立つことを確認する。
【０５１２】
[別記述E]
$\alpha=1,\ldots,\lambda$に関して順番に、計算者
【０５１３】
【数１９７】

$$u_{\alpha}$$

【０５１４】
は以下の処理を行う。
【０５１５】

【数１９８】

$$u_{\alpha}$$

【０５１６】
は、
【０５１７】
【数１９９】

$$\Sigma_{h=0,1/3,2/3}\ \sigma^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi} = s^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} \bmod q$$

$$\Sigma_{h=0,1/3,2/3}\ \tau^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi} = t^{(\alpha)\beta bc}{}_{[k]\mu,\nu,\xi} \bmod q$$

【０５１８】
なる
【０５１９】
【数２００】

$$\{\sigma^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi},\ \tau^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi},\}_{k=1,\ldots,m;\beta=1,\ldots,\lambda;h=2/3,1/3,0;b,c,\mu,\nu,\xi\in\{0,1\}}$$

【０５２０】
をZ/qZから一様無作為に選び，
全てのk=1,...,m、全ての
【０５２１】
【数２０１】

$$b,c,\mu,\nu,\xi\in\{0,1\}$$

【０５２２】
に関して，
【０５２３】

【数２０２】

$$A^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-1)bc}{}_{[k]\mu\square\pi(i),\nu,\xi} + [\sigma^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi}]G$$

$$B^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-1)bc}{}_{[k]\mu\square\pi(i),\nu,\xi} + [\sigma^{(\alpha-2/3)bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

$$C^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-1)\beta\ bc}{}_{[k]\mu\square\pi(i),\nu\ \xi} + [\tau^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}]G$$

$$D^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-1)\beta\ bc}{}_{[k]\mu\square\pi(i),\nu,\xi} + [\tau^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

$$A^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-2/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi}]G$$

$$B^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-2/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha-1/3)bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

$$C^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}]G$$

$$D^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-2/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

$$A^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} = A^{(\alpha-1/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha)bc}{}_{[k]\mu,\nu,\xi}]G$$

$$B^{(\alpha)bc}{}_{[k]\mu,\nu,\xi} = B^{(\alpha-1/3)bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\sigma^{(\alpha)bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

$$C^{(\alpha)\beta\ bc}{}_{[k]\mu,\nu,\xi} = C^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha)\beta\ bc}{}_{[k]\mu,\nu,\xi}]G$$

$$D^{(\alpha)\beta\ bc}{}_{[k]\mu,\nu,\xi} = D^{(\alpha-1/3)\beta\ bc}{}_{[k]\mu,\nu\square\pi(j),\xi} + [\tau^{(\alpha)\beta\ bc}{}_{[k]\mu,\nu,\xi}](Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z)$$

【０５２４】
を生成する。
【０５２５】
次に、全てのk=1,...,m、全てのβ=1,...,λ、全てのh=2/3,1/3,0、全ての
【０５２６】
【数２０３】

$$b,c,\mu,\nu,\xi \in \{0,1\}$$

【０５２７】
に関して、
【０５２８】

【数２０４】

$$\sigma^{\prime}(\alpha-h)bc_{[k]\mu,\nu,\xi},\ \tau^{\prime}(\alpha-h)\beta bc_{[k]\mu,\nu,\xi},$$

【０５２９】
をZ/qZから一様無作為に選び，
全てのk=1,...,m、全てのβ=1,...,λ、全ての
【０５３０】
【数２０５】

$$b,c,\mu,\nu,\xi \in \{0,1\}$$

【０５３１】
に関して，
【０５３２】

【数２０６】

$$A'^{(\alpha-2/3)bc}{}_{[k]}\pi(i),\mu,\nu,\xi = A^{(\alpha-1)bc}{}_{[k]}\mu\square\pi(i),\nu,\xi + [\sigma'^{(\alpha-2/3)bc}{}_{[k]}\mu,\nu,\xi]G$$

$$B'^{(\alpha-2/3)bc}{}_{[k]}\pi(i):\mu,\nu,\xi = B^{(\alpha-1)bc}{}_{[k]}\mu\square\pi(i),\nu,\xi + [\sigma'^{(\alpha-2/3)bc}{}_{[k]}\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$$

$$C'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\pi(i),\mu,\nu,\xi = C^{(\alpha-1)\beta\ bc}{}_{[k]}\mu\square\pi(i),\nu\ \xi + [\tau'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\mu,\nu,\xi]G$$

$$D'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\pi(i),\mu,\nu,\xi = D^{(\alpha-1)\beta\ bc}{}_{[k]}\mu\square\pi(i),\nu,\xi + [\tau'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$$

$$A'^{(\alpha-1/3)bc}{}_{[k]}\pi(j)\mu,\nu,\xi = A^{(\alpha-2/3)bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\sigma'^{(\alpha-1/3)bc}{}_{[k]}\mu,\nu,\xi]G$$

$$B'^{(\alpha-1/3)bc}{}_{[k]}\pi(j)\mu,\nu,\xi = B^{(\alpha-2/3)bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\sigma'^{(\alpha-1/3)bc}{}_{[k]}\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$$

$$C'^{(\alpha-1/3)\beta\ bc}{}_{[k]}\pi(j)\mu,\nu,\xi = C^{(\alpha-2/3)\beta\ bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\tau'^{(\alpha-1/3)\ \beta\ bc}{}_{[k]}\mu,\nu,\xi]G$$

$$D'^{(\alpha-1/3)\beta\ bc}{}_{[k]}\pi(j)\mu,\nu,\xi = D^{(\alpha-2/3)\beta\ bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\tau'^{(\alpha-1/3)\ \beta\ bc}{}_{[k]}\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$$

$$A'^{(\alpha)bc}{}_{[k]}\pi(k)\mu,\nu,\xi = A^{(\alpha-1/3)bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\sigma'^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi]G$$

$$B'^{(\alpha)bc}{}_{[k]}\pi(k)\mu,\nu,\xi = B^{(\alpha-1/3)bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\sigma'^{(\alpha)bc}{}_{[k]}\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$$

$$C'^{(\alpha)\beta\ bc}{}_{[k]}\pi(k)\mu,\nu,\xi = C^{(\alpha-1/3)\beta\ bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\tau'^{(\alpha)\beta\ bc}{}_{[k]}\mu,\nu,\xi]G$$

$$D'^{(\alpha)\beta\ bc}{}_{[k]}\pi(k)\mu\ nu\xi = D^{(\alpha-1/3)\beta\ bc}{}_{[k]}\mu,\nu\square\pi(j),\xi + [\tau'^{(\alpha)\ \beta\ bc}{}_{[k]}\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)$$

【０５３３】
を生成する。
【０５３４】
さらに全てのk=m+1,...,m+n、全てのβ=1,...,λ、全ての
【０５３５】
【数２０７】

$$b,\xi \in \{0,1\}$$

【０５３６】
に関して、
【０５３７】

【数２０８】

$$s'^{(\alpha)b}{}_{[k]\xi}, t'^{(\alpha)b}{}_{[k]\xi},$$

【０５３８】
をZ/qZから一様無作為に選び，
全てのk=m+1,...,m+n,全ての
【０５３９】
【数２０９】

$$b,\xi \in \{0,1\}$$

【０５４０】
に関して、
【０５４１】
【数２１０】

$$A'^{(\alpha)b}{}_{[k]\pi(k),\xi} = A^{(\alpha-1)b}{}_{[k]\xi} \square \pi(k) + [s'^{(\alpha)b}{}_{[k]\xi}]G$$

$$B'^{(\alpha)b}{}_{[k]\pi(k),\xi} = B^{(\alpha-1)b}{}_{[k]\xi} \square \pi(k) + [s'^{(\alpha)b}{}_{[k]\xi}](Y\tilde{}^{b}{}_{[k]}+Z)$$

$$C'^{(\alpha)\beta b}{}_{[k]\pi(k)\xi} = C^{(\alpha-1)\beta b}{}_{[k]\xi} \square \pi(k) + [t'^{(\alpha)\beta b}{}_{[k]\xi}]G$$

$$D'^{(\alpha)\beta b}{}_{[k]\pi(k)\xi} = D^{(\alpha-1)\beta b}{}_{[k]\xi} \square \pi(k) + [t'^{(\alpha)\beta b}{}_{[k]\xi}](Y\tilde{}^{b}{}_{[k]}+Z)$$

【０５４２】
を生成する。
さらに全てのk=1,...,l,全ての
【０５４３】
【数２１１】

$$b,\xi \in \{0,1\}$$

【０５４４】
に関して、
【０５４５】
【数２１２】

$$s\dagger'^{(\alpha)b}{}_{[k]\xi},$$

【０５４６】
をZ/qZから一様無作為に選び、
全てのk=1,...,l,全ての
【０５４７】
【数２１３】

$$b,\xi \in \{0,1\}$$

【０５４８】
に関して、
【０５４９】
【数２１４】

$$A^{\dagger\prime(\alpha)b}{}_{[k]}\pi(k)\xi = A^{\dagger(\alpha-1)b}{}_{[k]}\xi \square \pi(k)^{+}\,[s^{\dagger\prime(\alpha)b}{}_{[k]}\xi]G$$

$$B^{\dagger\prime(\alpha)b}{}_{[k]}\pi(k)\xi = B^{\dagger(\alpha-1)\,b}{}_{[k]}\xi \square \pi(k)^{+}\,[s^{\dagger\prime(\alpha)b}{}_{[k]}\xi](Y^{b}{}_{[k]}+Z)$$

【０５５０】
を生成する。
【０５５１】
次に、全てのk=1,...,m、全てのh=2/3,1/3,0に関して、
【０５５２】
【数２１５】

$$\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1,$$

【０５５３】
をZ/qZから一様無作為に選ぶ。
【０５５４】
次に、全てのk=1,...,m、全てのβ=1,...,λ、全ての
【０５５５】
【数２１６】

$$b,c,\mu,\nu,\xi \in \{0,1\}$$

【０５５６】
に関して、
【０５５７】
【数２１７】

$$\sigma^{\prime\prime(\alpha-2/3)bc}{}_{[k]}\,\pi(i)\square 1,\mu,\nu,\xi,\ \sigma^{\prime\prime(\alpha-1/3)bc}{}_{[k]}\,\pi(j)\square 1,\mu,\nu,\xi,\ \sigma^{\prime\prime(\alpha)bc}{}_{[k]}\,\pi(k)\square 1,\mu,\nu,\xi,\ \tau^{\prime\prime(\alpha-2/3)\beta\ bc}{}_{[k]}\,\pi(i)\square 1,\mu,\nu,\xi,\ \tau^{\prime\prime(\alpha-1/3)\beta\ bc}{}_{[k]}\,\pi(j)\square 1,\mu,\nu,\xi,\ \tau^{\prime\prime(\alpha)\beta bc}{}_{[k]}\,\pi(k)\square 1,\mu,\nu,\xi$$

【０５５８】
をZ/qZから一様無作為に選ぶ。
【０５５９】
次に、全てのk=m+1,...,m+n、全てのβ=1,...,λ、全ての
【０５６０】
【数２１８】

$$b,\xi \in \{0,1\}$$

【０５６１】
に関して,
【０５６２】

【数２１９】

$$s''(\alpha)b_{[k]}\ \pi(k)\square 1,\xi,t''(\alpha)\beta b_{[k]}\ \pi(k)\square 1,\xi$$

【０５６３】
をZ/qZから一様無作為に選ぶ。
次に、全てのk=1,...,l、全ての
【０５６４】
【数２２０】

$$b,\xi\in\{0,1\}$$

【０５６５】
に関して、
【０５６６】
【数２２１】

$$s\dagger''(\alpha)b_{[k]}\ \pi(k)\square 1,\xi,t\dagger''(\alpha)b_{[k]}\ \pi(k)\square 1,\xi$$

【０５６７】
をZ/qZから一様無作為に選ぶ。
【０５６８】
次に、全てのk=1,...,m、全てのβ=1,...,λ、全ての
【０５６９】
【数２２２】

$$b,c,\mu,\nu,\xi\in\{0,1\}$$

【０５７０】
に関して、
【０５７１】

【数２２３】

$$A'^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ A^{(\alpha-1)bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$$

$$B'^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-2/3)bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ B^{(\alpha-1)bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$$

$$C'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ C^{(\alpha-1)\beta bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$$

$$D'^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \pi(i)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(i)\square 1]\ D^{(\alpha-1)\beta bc}{}_{[k]}\ \mu\square\pi(i),\nu,\xi$$

$$A'^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ A^{(\alpha-2/3)bc}{}_{[k]}\ \mu,\nu\square\pi(j),\ \xi$$

$$B'^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha-1/3)bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ B^{(\alpha-2/3)bc}{}_{[k]}\ \mu,\nu\square\pi(j),\xi$$

$$C'^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ C^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \mu,\nu\square\pi(j),\ \xi$$

$$D'^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \pi(j)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(j)\square 1]\ D^{(\alpha-2/3)\beta\ bc}{}_{[k]}\ \mu,\nu\square\pi(j),\xi$$

$$A'^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ A^{(\alpha-1/3)bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$$

$$B'^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\sigma''^{(\alpha)bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ B^{(\alpha-1/3)bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$$

$$C'^{(\alpha)\beta bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha)\beta bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]G - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ C^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$$

$$D'^{(\alpha)\beta bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi = [\tau''^{(\alpha)\beta bc}{}_{[k]}\ \pi(k)\square 1,\mu,\nu,\xi]\ (Y^{b}{}_{[i]}+Y^{c}{}_{[j]}+Z) - [\theta^{(\alpha)}{}_{[k]}\pi(k)\square 1]\ D^{(\alpha-1/3)\beta\ bc}{}_{[k]}\ \mu,\nu,\xi\square\pi(k)$$

【０５７２】

を生成する。

【０５７３】

次に、全てのk=m+1,...,m+n、全てのβ=1,...,λ、全ての

【０５７４】

【数２２４】

$$b,\xi\in\{0,1\}$$

【０５７５】
に関して、
【０５７６】
【数２２５】

$$A'^{(\alpha)b}_{[k]\ \pi(i)\square 1,\xi} = [s''^{(\alpha-1)b}_{[k]\ \pi(i)\square 1,\xi}]G - [\theta^{(\alpha)}_{[k]\pi(i)\square 1}]\ A^{(\alpha-1)b}_{[k]\ \xi\square\pi(i)}$$

$$B'^{(\alpha)b}_{[k]\ \pi(i)\square 1,\xi} = [s''^{(\alpha-1)b}_{[k]\ \pi(i)\square 1,\xi}](Y^{\sim b}_{[k]} + Z) - [\theta^{(\alpha)}_{[k]\pi(i)\square 1}]\ B^{(\alpha-1)b}_{[k]\ \xi\square\pi(i)}$$

$$C'^{(\alpha)\beta b}_{[k]\ \pi(i)\square 1,\xi} = [t''^{(\alpha-1)\beta b}_{[k]\ \pi(i)\square 1,\xi}]G - [\theta^{(\alpha)}_{[k]\pi(i)\square 1}]\ C^{(\alpha-1)\beta b}_{[k]\ \xi\square\pi(i)}$$

$$D'^{(\alpha)\beta b}_{[k]\ \pi(i)\square 1,\xi} = [t''^{(\alpha-1)\beta b}_{[k]\ \pi(i)\square 1,\xi}](Y^{\sim b}_{[k]} + Z) - [\theta^{(\alpha)}_{[k]\pi(i)\square 1}]\ D^{(\alpha-1)\beta b}_{[k]\ \xi\square\pi(i)}$$

【０５７７】
を生成する。
【０５７８】
次に、全てのk=1,...,l、全ての
【０５７９】
【数２２６】

$$b,\xi \in \{0,1\}$$

【０５８０】
に関して、
【０５８１】
【数２２７】

$$A^{\dagger'^{(\alpha)b}}_{[k]\ \pi(i)\square 1,\xi} = [s^{\dagger''^{(\alpha-1)b}}_{[k]\ \pi(i)\square 1,\xi}]G - [\theta^{(\alpha)}_{[k]\pi(i)\square 1}]\ A^{\dagger(\alpha-1)b}_{[k]\ \xi\square\pi(i)}$$

$$B^{\dagger'^{(\alpha)b}}_{[k]\ \pi(i)\square 1,\xi} = [s^{\dagger''^{(\alpha-1)b}}_{[k]\ \pi(i)\square 1,\xi}](Y^{b}_{[k]} + Z) - [\theta^{(\alpha)}_{[k]\pi(i)\square 1}]\ B^{\dagger(\alpha-1)b}_{[k]\ \xi\square\pi(i)}$$

【０５８２】
を生成する。
【０５８３】
次に、
【０５８４】

【数２２８】

$S = \{ E,G,$

$\{$

$A^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}, B^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi}, C^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi}, D^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi},$

$A'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}, B'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi}, C'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}, D'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi}$

$k=1,...,m;h=2/3,1/3,0;\beta=1,...,\lambda;b,c,\mu,\nu,\xi,\zeta\in\{0,1\}$

$\{$

$A^{(\alpha)b}{}_{[k]\xi}, B^{(\alpha)b}{}_{[k]\xi}, C^{(\alpha)\beta b}{}_{[k]\xi}, D^{(\alpha)\beta b}{}_{[k]\xi},$

$A'^{(\alpha)b}{}_{[k]\zeta,\xi}, B'^{(\alpha)b}{}_{[k]\zeta,\xi}, C'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}, D'^{(\alpha)\beta b}{}_{[k]\zeta,\xi}$

$k=m+1,...,m+n;\beta=1,...,\lambda;b,\xi,\zeta\in\{0,1\}\}$

$\{$

$A^{\dagger(\alpha)b}{}_{[k]\xi}, B^{\dagger(\alpha)b}{}_{[k]\xi}$

$A^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}, B^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$

$k=1,...,l;b,\xi,\zeta\in\{0,1\}\}$

【０５８５】
を生成する。
【０５８６】
次に、各u_αは、全てのk=1,...,m+nに関して
【０５８７】
【数２２９】

$$\theta^{(\alpha)}{}_{[k]} = \mathrm{Hash}(E,G,k,S)$$

【０５８８】
を生成する。
【０５８９】
次に、全てのk=1,...,m+nに関して
【０５９０】
【数２３０】

$$\theta^{(\alpha)}{}_{[k]\pi(i)} = \theta^{(\alpha)}{}_{[k]} - \theta^{(\alpha)}{}_{[k]\pi(i)\square 1}$$

【０５９１】
を生成する。次に、全てのk=1,...,m、全てのβ=1,...,λ、全てのh=2/3,1/3,0、全ての
【０５９２】
【数２３１】

$$b,c,\mu,\nu,\xi \in \{0,1\}$$

【０５９３】
に関して、
【０５９４】
【数２３２】

$$\sigma''(\alpha-h)bc_{[k]\pi(i),\mu,\nu,\xi} = \theta(\alpha)_{[k]\pi(i)}\,\sigma(\alpha-2/3)bc_{[k]\mu,\nu,\xi} + \sigma'(\alpha-2/3)bc_{[k]\mu,\nu,\xi} \bmod q$$

$$\tau''(\alpha-h)\beta\, bc_{[k]\pi(i),\mu,\nu,\xi} = \theta(\alpha)_{[k]\pi(i)}\,\tau(\alpha-2/3)\beta\; bc_{[k]\mu,\nu,\xi} + \tau'(\alpha-2/3)\beta\; bc_{[k]\mu,\nu,\xi} \bmod q$$

【０５９５】
を生成する。
【０５９６】
次に、全てのk=m+1,...,m+n、全てのβ=1,...,λ、全ての
【０５９７】
【数２３３】

$$b,\xi \in \{0,1\}$$

【０５９８】
に関して,
【０５９９】
【数２３４】

$$s''(\alpha)b_{[k]\pi(i)\xi} = \theta(\alpha)_{[k]\pi(i)}\,s(\alpha-1)b_{[k]\xi} + s'(\alpha-1)b_{[k]\xi} \bmod q$$

$$t''(\alpha)\beta\, b_{[k]\pi(i)\xi} = \theta(\alpha)_{[k]\pi(i)}\,t(\alpha-1)\beta\, b_{[k]\xi} + t'(\alpha-1)b_{[k]\xi} \bmod q$$

【０６００】
を生成する。
【０６０１】
次に、全てのk=1,...,l、全ての
【０６０２】
【数２３５】

$$b,\xi \in \{0,1\}$$

【０６０３】
に関して,
【０６０４】

【数２３６】

$$s^{\dagger''(\alpha)b}{}_{[k]\pi(i)\xi} = \theta(\alpha)_{[k]\pi(i)}\, s^{\dagger(\alpha-1)b}{}_{[k]\xi} + s^{\dagger'(\alpha-1)b}{}_{[k]\xi} \bmod q$$

【０６０５】
を生成する。
【０６０６】
最後に、全ての
【０６０７】
【数２３７】

$$k=1,\ldots,m;h=2/3,1/3,0;\beta=1,\ldots,\lambda;b,c,\mu,\nu,\xi,\zeta\in\{0,1\}$$

【０６０８】
に関する
【０６０９】
【数２３８】

$$A^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi},\ B^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi},\ C^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi},\ D^{(\alpha-h)\beta bc}{}_{[k]\mu,\nu,\xi},$$

$$A'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi},\ B'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi},\ C'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi},\ D'^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi},$$

$$\sigma''^{(\alpha)b}{}_{[k]\zeta,\xi},\ \tau''^{(\alpha)\beta b}{}_{[k]\zeta,\xi},$$

【０６１０】
及び、全ての
【０６１１】
【数２３９】

$$k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda;b,\xi,\zeta\in\{0,1\}$$

【０６１２】
に関する
【０６１３】
【数２４０】

$$A^{(\alpha)b}{}_{[k]\xi},\ B^{(\alpha)b}{}_{[k]\xi},\ C^{(\alpha)\beta b}{}_{[k]\xi},\ D^{(\alpha)\beta b}{}_{[k]\xi},$$

$$A'^{(\alpha)b}{}_{[k]\zeta,\xi},\ B'^{(\alpha)b}{}_{[k]\zeta,\xi},\ C'^{(\alpha)\beta b}{}_{[k]\zeta,\xi},\ D'^{(\alpha)\beta b}{}_{[k]\zeta,\xi},$$

$$s''^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi},\ t''^{(\alpha-h)\beta bc}{}_{[k]\zeta,\mu,\nu,\xi},$$

【０６１４】
及び、全ての
【０６１５】

【数２４１】

$$k=1,\ldots,l;b,\xi,\zeta\in\{0,1\}$$

【０６１６】
に関する
【０６１７】
【数２４２】

$$A^{\dagger(\alpha)b}{}_{[k]\xi},\ B^{\dagger(\alpha)b}{}_{[k]\xi},$$

$$A^{\dagger\prime(\alpha)b}{}_{[k]\zeta,\xi},\ B^{\dagger\prime(\alpha)b}{}_{[k]\zeta,\xi},$$

$$s^{\dagger\prime\prime(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi},$$

及び，全てのk=1,...,m+n に関する

$$\theta(\alpha)_{[k]\zeta}$$

【０６１８】
を証明とする。上記証明の検証方法は以下の通り。
【０６１９】
検証者は、
【０６２０】

【数２４３】

$$S = [\, E,G,$$

$$\{$$

$$A^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi},\ B^{(\alpha-h)bc}{}_{[k]\mu,\nu,\xi},\ C^{(\alpha-h)\beta\,bc}{}_{[k]\mu,\nu,\xi},\ D^{(\alpha-h)\beta\,bc}{}_{[k]\mu,\nu,\xi},$$

$$A'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi},\ B'^{(\alpha-h)bc}{}_{[k]\zeta,\mu,\nu,\xi},\ C'^{(\alpha-h)\beta\,bc}{}_{[k]\zeta,\mu,\nu,\xi},\ D'^{(\alpha-h)\beta\,bc}{}_{[k]\zeta,\mu,\nu,\xi}$$

$$\}_{k=1,\ldots,m;h=2/3,1/3,0;\beta=1,\ldots,\lambda\,;\,b,c,\mu,\nu,\xi,\zeta\in[0,1]}$$

$$\{$$

$$A^{(\alpha)b}{}_{[k]\xi},\ B^{(\alpha)b}{}_{[k]\xi},\ C^{(\alpha)\beta\,b}{}_{[k]\xi},\ D^{(\alpha)\beta\,b}{}_{[k]\xi},$$

$$A'^{(\alpha)b}{}_{[k]\zeta,\xi},\ B'^{(\alpha)b}{}_{[k]\zeta,\xi},\ C'^{(\alpha)\beta\,b}{}_{[k]\zeta,\xi},\ D'^{(\alpha)\beta\,b}{}_{[k]\zeta,\xi}$$

$$\}_{k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda\,;b,\xi,\zeta\in[0,1]}\}$$

$$\{$$

$$A^{\dagger(\alpha)b}{}_{[k]\xi},\ B^{\dagger(\alpha)b}{}_{[k]\xi}$$

$$A^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi},\ B^{\dagger'(\alpha)b}{}_{[k]\zeta,\xi}$$

$$k=1,\ldots,l;b,\xi,\zeta\in[0,1]\}$$

【０６２１】
を生成し、各u_αは、全てのk=1,...,m+nに関して
【０６２２】
【数２４４】

$$\theta^{(\alpha)}{}_{[k]} = \mathrm{Hash}(E,G,k,\ S)$$

【０６２３】
を生成し、全てのk=1,...,mに関して、
【０６２４】
【数２４５】

$$\theta^{(\alpha)}{}_{[k]0} + \theta^{(\alpha)}{}_{[k]1} = \theta^{(\alpha)}{}_{[k]}$$

【０６２５】
が成り立つことを確認する。検証者は次に、
【０６２６】

【数２４６】

$$k=1,\ldots,m;h=2/3,1/3,0;\beta=1,\ldots,\lambda;b,c,\mu,\nu,\xi,\zeta\in\{0,1\}$$

【０６２７】
に関して
【０６２８】
【数２４７】

$$[\sigma''(\alpha-2/3)bc_{[k]}\zeta,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\zeta](A(\alpha-2/3)bc_{[k]}\mu,\nu,\xi-A(\alpha-1)bc_{[k]}\mu\square\zeta,\nu,\xi)-A'(\alpha-2/3)bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\sigma''(\alpha-2/3)bc_{[k]}\zeta,\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)=[\theta(\alpha)_{[k]}\zeta](B(\alpha-2/3)bc_{[k]}\mu,\nu,\xi-B(\alpha-1)bc_{[k]}\mu\square\zeta,\nu,\xi)-B'(\alpha-2/3)bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\tau''(\alpha-2/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\zeta](C(\alpha-2/3)\beta\ bc_{[k]}\mu,\nu,\xi-C(\alpha-1)\beta\,bc_{[k]}\mu\square\zeta,\nu,\xi)-C'(\alpha-2/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\tau''(\alpha-2/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)=[\theta(\alpha)_{[k]}\zeta](D(\alpha-2/3)\beta\ bc_{[k]}\mu,\nu,\xi-D(\alpha-1)\beta\,bc_{[k]}\mu\square\zeta,\nu,\xi)-D'(\alpha-2/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\sigma''(\alpha-1/3)bc_{[k]}\zeta,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\zeta](A(\alpha-1/3)bc_{[k]}\mu,\nu,\xi-A(\alpha-2/3)bc_{[k]}\mu\square\zeta,\nu,\xi)-A'(\alpha-1/3)bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\sigma''(\alpha-1/3)bc_{[k]}\zeta,\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)=[\theta(\alpha)_{[k]}\zeta](B(\alpha-2/3)bc_{[k]}\mu,\nu,\xi-B(\alpha-2/3)bc_{[k]}\mu\square\zeta,\nu,\xi)-B'(\alpha-1/3)bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\tau''(\alpha-1/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\zeta](C(\alpha-1/3)\beta\ bc_{[k]}\mu,\nu,\xi-C(\alpha-2/3)\beta\ bc_{[k]}\mu\square\zeta,\nu,\xi)-C'(\alpha-1/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\tau''(\alpha-1/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)=[\theta(\alpha)_{[k]}\zeta](D(\alpha-1/3)\beta\ bc_{[k]}\mu,\nu,\xi-D(\alpha-2/3)\beta\ bc_{[k]}\mu\square\zeta,\nu,\xi)-D'(\alpha-1/3)\beta\ bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\sigma''(\alpha)bc_{[k]}\zeta,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\zeta](A(\alpha)bc_{[k]}\mu,\nu,\xi-A(\alpha-1/3)bc_{[k]}\mu\square\zeta,\nu,\xi)-A'(\alpha)bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\sigma''(\alpha)bc_{[k]}\zeta,\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)=[\theta(\alpha)_{[k]}\zeta](B(\alpha-1/3)bc_{[k]}\mu,\nu,\xi-B(\alpha-2/3)bc_{[k]}\mu\square\zeta,\nu,\xi)-B'(\alpha)bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\tau''(\alpha)\beta\,bc_{[k]}\zeta,\mu,\nu,\xi]G=[\theta(\alpha)_{[k]}\zeta](C(\alpha)\beta\,bc_{[k]}\mu,\nu,\xi-C(\alpha-1/3)\beta\ bc_{[k]}\mu\square\zeta,\nu,\xi)-C'(\alpha)\beta\,bc_{[k]}\zeta,\mu,\nu,\xi$$

$$[\tau''(\alpha)\beta\,bc_{[k]}\zeta,\mu,\nu,\xi](Y^b{}_{[i]}+Y^c{}_{[j]}+Z)=[\theta(\alpha)_{[k]}\zeta](D(\alpha)\beta\,bc_{[k]}\mu,\nu,\xi-D(\alpha-1/3)\beta\ bc_{[k]}\mu\square\zeta,\nu,\xi)-D'(\alpha)\beta\,bc_{[k]}\zeta,\mu,\nu,\xi$$

【０６２９】
が成り立つことを確認する。
【０６３０】
検証者は次に、
【０６３１】
【数２４８】

$$k=m+1,\ldots,m+n;\beta=1,\ldots,\lambda;b,\xi,\zeta\in\{0,1\}$$

【０６３２】
に関して
【０６３３】
【数２４９】

$$[s''(\alpha)b_{[k]\zeta,\xi}]G=[\theta(\alpha)_{[k]\zeta}](A(\alpha)b_{[k]\xi}-A(\alpha-1)b_{[k]\xi\square\zeta})-A'(\alpha)b_{[k]\zeta,\xi}$$

$$[s''(\alpha)b_{[k]\zeta,\xi}](Y\tilde{}b_{[k]}+Z)=[\theta(\alpha)_{[k]\zeta}](B(\alpha)b_{[k]\xi}-B(\alpha-1)b_{[k]\xi\square\zeta})-B'(\alpha)b_{[k]\zeta,\xi}$$

$$[t''(\alpha)\beta b_{[k]\zeta,\xi}]G=[\theta(\alpha)_{[k]\zeta}](C(\alpha)\beta b_{[k]\xi}-C(\alpha-1)\beta b_{[k]\xi\square\zeta})-C'(\alpha)\beta b_{[k]\zeta,\xi}$$

$$[t''(\alpha)\beta b_{[k]\zeta,\xi}](Y\tilde{}b_{[k]}+Z)=[\theta(\alpha)_{[k]\zeta}](D(\alpha)\beta b_{[k]\xi}-D(\alpha-1)\beta b_{[k]\xi\square\zeta})-D'(\alpha)\beta b_{[k]\zeta,\xi}$$

【０６３４】
が成り立つことを確認する。検証者は次に、
【０６３５】
【数２５０】

$$k=1,\ldots,l;b,\xi,\zeta\in\{0,1\}$$

【０６３６】
に関して
【０６３７】
【数２５１】

$$[s\dagger''(\alpha)b_{[k]\zeta,\xi}]G=[\theta(\alpha)_{[k]\zeta}](A\dagger(\alpha)b_{[k]\xi}-A\dagger(\alpha-1)b_{[k]\xi\square\zeta})-A\dagger'(\alpha)b_{[k]\zeta,\xi}$$

$$[s\dagger''(\alpha)b_{[k]\zeta,\xi}](Yb_{[k]}+Z)=[\theta(\alpha)_{[k]\zeta}](B\dagger(\alpha)b_{[k]\xi}-B\dagger(\alpha-1)b_{[k]\xi\square\zeta})-B'(\alpha)b_{[k]\zeta,\xi}$$

【０６３８】
が成り立つことを確認する。
【０６３９】
[別記述F]
証明者(計算者)
【０６４０】

【数２５２】

$$u_{\alpha} \text{ は, 全てのk=1,...,m+n, 全てのb,c} \in \{0,1\}$$

【０６４１】
に関して、全ての証明者(計算者)
【０６４２】
【数２５３】

$$\{u_{\alpha}\}_{\alpha=1,\ldots,\lambda}$$

【０６４３】
は、
【０６４４】
【数２５４】

$$z'(\alpha) \in_R Z/qZ$$

【０６４５】
を一様無作為に生成し,
【０６４６】
【数２５５】

$$Z'(\alpha) = [z'(\alpha)]G$$

【０６４７】
を生成し、全てのk=1,...,m、全ての
【０６４８】
【数２５６】

$$b,c \in \{0,1\}$$

【０６４９】
、全てのβ=1,...,λに関して
【０６５０】
【数２５７】

$$A'(\lambda)\alpha bc_{[k]000} = [z'(\alpha)]A(\lambda)bc_{[k]000}$$

$$C'(\lambda)\alpha\beta bc_{[k]000} = [z'(\alpha)]C(\lambda)\alpha bc_{[k]000}$$

【０６５１】
を生成し、全てのk=m+1,...,m+n、全ての
【０６５２】
【数２５８】

$$b \in \{0,1\}$$

【０６５３】

、全てのβ=1,...,λに関して
【０６５４】
【数２５９】

$$A'(\lambda)\alpha b_{[k]0}=[z'(\alpha)]A(\lambda)b_{[k]0}$$

$$C'(\lambda)\alpha\beta b_{[k]0}=[z'(\alpha)]C(\lambda)\alpha b_{[k]0}$$

【０６５５】
を生成し、全てのk=1,...,l、全ての
【０６５６】
【数２６０】

$$b\in\{0,1\}$$

【０６５７】
に関して
【０６５８】
【数２６１】

$$A^{\dagger'}(\lambda)\alpha b_{[k]0}=[z'(\alpha)]A^{\dagger}(\lambda)b_{[k]0}$$

【０６５９】
を生成する。
【０６６０】

【数２６２】

$$S = \{ \{ A(\lambda)bc_{[k]000}, C(\lambda)\beta bc_{[k]000}, \}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{ A(\lambda)b_{[k]0}, C(\lambda)\beta b_{[k]0} \}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{ A\dagger(\lambda)b_{[k]0} \}_{k=1,...,l;b=0,1},$$

$$\{ A\sharp(\lambda)\alpha bc_{[k]000}, C\sharp(\lambda)\alpha\beta bc_{[k]000} \}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{ A\sharp(\lambda)\alpha b_{[k]0}, C\sharp(\lambda)\alpha \text{ beta } b_{[k]0}k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda,$$

$$\{ A\dagger\sharp(\lambda)\alpha b_{[k]0} \}_{k=1,...,l;b=0,1},$$

$$\{Z'(\alpha)\},$$

$$\{ A'(\lambda)\alpha bc_{[k]000}, C'(\lambda)\alpha\beta bc_{[k]000} \}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{ A'(\lambda)\alpha b_{[k]0}, C'(\lambda)\alpha\beta b_{[k]0} \}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{ A\dagger'(\lambda)\alpha b_{[k]0} \}_{k=1,...,l;b=0,1}, .] \}$$

【０６６１】
を生成し、さらに
【０６６２】
【数２６３】

$$\theta = \text{Hash}(E,G,S) \bmod q$$

【０６６３】
を生成する。さらに
【０６６４】
【数２６４】

$$z''(\alpha) = z(\alpha)\theta + z'(\alpha) \bmod q$$

【０６６５】
を生成する。証明者は、
【０６６６】

【数２６５】

$$Z'(\alpha),\{A'(\lambda)\alpha bc_{[k]000}, C'(\lambda)\alpha\beta bc_{[k]000}\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{A'(\lambda)\alpha b_{[k]0}, C'(\lambda)\alpha\beta b_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{A\dagger'(\lambda)\alpha b_{[k]0}\}_{k=1,...,l;b=0,1},$$

$$z''(\alpha)$$

【０６６７】
を証明とする。上記証明の検証方法は以下の通り。
【０６６８】
検証者は、
【０６６９】
【数２６６】

$$S=[\{A(\lambda)bc_{[k]000}, C(\lambda)\beta bc_{[k]000},\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{A(\lambda)b_{[k]0}, C(\lambda)\beta b_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{A\dagger(\lambda)b_{[k]0}\}_{k=1,...,l;b=0,1},$$

$$\{A\ddagger(\lambda)\alpha bc_{[k]000}, C\ddagger(\lambda)\alpha\beta bc_{[k]000}\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{A\ddagger(\lambda)\alpha b_{[k]0}, C\ddagger(\lambda)\alpha\beta b_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{A\dagger\ddagger(\lambda)\alpha b_{[k]0}\}_{k=1,...,l;b=0,1},$$

$$\{Z'(\alpha)\},$$

$$\{A'(\lambda)\alpha bc_{[k]000}, C'(\lambda)\alpha\beta bc_{[k]000}\}_{k=1,...,m;b,c=0,1;\beta=1,...,\lambda},$$

$$\{A'(\lambda)\alpha b_{[k]0}, C'(\lambda)\alpha\beta b_{[k]0}\}_{k=m+1,...,m+n;b=0,1;\beta=1,...,\lambda},$$

$$\{A\dagger'(\lambda)\alpha b_{[k]0}\}_{k=1,...,l;b=0,1},.\}]$$

【０６７０】
を生成し、さらに
【０６７１】
【数２６７】

$$\theta = \mathrm{Hash}(E,G,S) \bmod q$$

【０６７２】
を計算して、
【０６７３】

【数２６８】

$$[z''(\alpha)]G = Z'(\alpha) + [\theta]Z(\alpha)$$

【０６７４】
全ての
【０６７５】
【数２６９】

$$k=1,\ldots,m,\ b,c \in \{0,1\},\ \beta=1,\ldots,\lambda$$

【０６７６】
に関して
【０６７７】
【数２７０】

$$[z''(\alpha)]\,A(\lambda)bc_{[k]000} = A'(\lambda)\alpha bc_{[k]000} + [\theta]\,A\sharp(\lambda)\alpha bc_{[k]000}$$

$$[z''(\alpha)]C(\lambda)\beta bc_{[k]000} = C'(\lambda)\alpha\beta bc_{[k]000} + [\theta]C\sharp(\lambda)\alpha\beta bc_{[k]000}$$

【０６７８】
全ての
【０６７９】
【数２７１】

$$k=m+1,\ldots,m+n,\ b \in \{0,1\},\ \beta=1,\ldots,\lambda$$

【０６８０】
に関して
【０６８１】
【数２７２】

$$[z''(\alpha)]A(\lambda)b_{[k]0} = A'(\lambda)\alpha b_{[k]0} + [\theta]A\sharp(\lambda)\alpha b_{[k]0}$$

$$[z''(\alpha)]C(\lambda)\beta b_{[k]0} = C'(\lambda)\alpha\beta b_{[k]0} + [\theta]C\sharp(\lambda)\alpha\beta b_{[k]0}$$

【０６８２】
全ての
【０６８３】
【数２７３】

$$k=1,\ldots,l,\ b \in \{0,1\}$$

【０６８４】
に関して
【０６８５】

【数２７４】

$$[z''(\alpha)]A^{\dagger}(\lambda)b_{[k]0}=A^{\dagger'}(\lambda)\alpha b_{[k]0}+[\theta]A^{\dagger\sharp}(\lambda)\alpha b_{[k]0}$$

【０６８６】
を確認する。
【０６８７】
［別記述G］
計算者
【０６８８】
【数２７５】

$$u(\alpha)$$

【０６８９】
は
【０６９０】
【数２７６】

$$z'(\alpha)\in_R Z/qZ$$

【０６９１】
を一様無作為に生成し、全てのk=1,...,lに関して，
【０６９２】
【数２７７】

$$A^{\dagger'}{}_{[k]}=[z'(\alpha)]A^{\dagger b\lceil k\rfloor}{}_{[k]}$$

【０６９３】
を生成する。証明者は、
【０６９４】
【数２７８】

$$S=\{\{A^{\dagger b\lceil k\rfloor}{}_{[k]}\}_{k=1,...,l},$$

$$\{A^{\dagger\sharp}{}_{[k]}\}_{k=1,...,l},$$

$$\{A^{\dagger'}{}_{[k]}\}_{k=1,...,l}\}$$

【０６９５】
を生成して、
【０６９６】
【数２７９】

$$\theta=\mathrm{Hash}(E,G,S)\bmod q$$

【０６９７】
を生成する。証明者は
【０６９８】

【数２８０】

$$z''(\alpha) = \theta\ z(\alpha) + z'(\alpha) \bmod q$$

【０６９９】
を生成する。証明者
【０７００】
【数２８１】

$$\{ A^{\dagger\sharp}{}_{[k]} \}_{k=1,\ldots,l}, z''(\alpha)$$

【０７０１】
を証明とする。上記証明の検証方法は以下の通り。検証者は、
【０７０２】
【数２８２】

$$S = \{ \{ A^{\dagger b\lceil k \rfloor}{}_{[k]} \}_{k=1,\ldots,l},$$

$$\{ A^{\dagger\sharp}{}_{[k]} \}_{k=1,\ldots,l},$$

$$\{ A^{\dagger'}{}_{[k]} \}_{k=1,\ldots,l} \}$$

【０７０３】
を生成して，
【０７０４】
【数２８３】

$$\theta = \mathrm{Hash}(E, G, S) \bmod q$$

【０７０５】
を生成する。検証者は
【０７０６】
【数２８４】

$$[z''(\alpha)] A^{\dagger b\lceil k \rfloor}{}_{[k]} = A^{\dagger'}{}_{[k]} + [\theta]\, A^{\dagger\sharp}{}_{[k]}$$

【０７０７】
を確認できたら証明を受理する。
【０７０８】
実施例２
本発明の第２の実施例について、図１４ないし図１８を用いて説明する。
【０７０９】
本実施例においては、図１４に示すように計算装置1401がN個あり、それぞれ計算装置1403を備えているものとする。以下ではこの計算機を順番に$U_1, \cdots, U_N$ と呼ぶことにする。記法の都合上、U_Nの事をU_0とも書く事にする。
【０７１０】
[方式の概略]
[データの流れ]
実施例２におけるデータの流れを図１６を参照して説明する。

【０７１１】
まず、計算装置1401のU_1は$DATA_0^0$を計算する。これを「0周目の計算」とよぶ(1701)。
【０７１２】
次に「一周目の計算」を行う。
【０７１３】
U_1は$DATA_0^0$から$DATA_1^1$を計算して、$DATA_1^1$をU_2に送る(1711)。
【０７１４】
次にU_2は$DATA_1^1$から$DATA_1^2$を計算し、$DATA_1^2$をU_3に送る(1712)。
【０７１５】
以下順にデータを送って行き、U_Nは$DATA_1^{N-1}$から$DATA_1^N$を計算し、$DATA_1^N$をU_1に送る(1710)。
ここまでが一周目の計算である。
【０７１６】
次に「二周目の計算」を行う。
【０７１７】
U_1は$DATA_1^N$から$DATA_2^1$を計算して、$DATA_2^1$をU_2に送る(1721)。
【０７１８】
次にU_2は$DATA_2^1$から$DATA_2^2$を計算し、$DATA_2^1$をU_3に送る(1722)。
【０７１９】
以下順にデータを送って行き、U_Nは$DATA_2^{N-1}$から$DATA_2^N$を計算し、$DATA_2^N$をU_1に送る(1720)。
ここまでが二周目の計算である。
【０７２０】
次に「三周目の計算」を行う。
【０７２１】
U_1は$DATA_2^N$から$DATA_3^1$を計算して、$DATA_2^1$をU_2に送る(1731)。
【０７２２】
以下順にデータを送って行き、U_Nが$DATA_3^{N-1}$から$DATA_3^N$を計算し終えたところでプロトコルが終了となる。
【０７２３】
[各計算装置1401の入出力]
次に各計算装置1401のやり取りするデータの入出力を図１４を参照して説明する。
【０７２４】
各計算装置1401には、回路の情報1404、および回路の部分入力1402が入力される。
【０７２５】
ここでは、回路の情報1404が表す回路の入力素子以外の素子のfan-inの数が2である場合に対し説明する。
【０７２６】
回路の入力素子wへの入力b_wはU_1、…、U_Nのいずれかが秘密裡に所有しているものとする。U_1の事をU_{N+1}とも書く事にする。
【０７２７】
U_1が秘密裡に所有している入力ビットの組が回路の部分入力1402である。
【０７２８】
回路の情報1404が表す回路の入力素子iを、いかなる入力が入ってもb_wを出力する素子だと思い直した回路を以下C[1]と表す。
【０７２９】
C[1]の全てのゲートのfan-inの数は2である。
【０７３０】
素子wの左下、右下のfan-inをそれぞれL(w)、R(w)と書く事にする。
【０７３１】

各計算装置1401に回路の情報1404、および回路の部分入力1402が入力されたら、まずU_lは後で説明する手順に従って0周目の計算を行う。

【０７３２】

１周目、２周目、３周目の計算での入出力は同様のデータ構造を持っている。i=1,2,3に対し、

ユーザU_lが第i周目の計算でU_{l+1}に送信するデータを$DATA_i^l$と表す事にする。$DATA_{i-1}^N$を$DATA_i^0$とも書く事にする。

【０７３３】

また、第0周目の計算でU_lが行った計算の計算結果を$DATA_0^l$と書く。

【０７３４】

$DATA_i^l$は、$DATA_i^l = DATA_i^{l-1} \,||\, BODY_i^l \,||\, PROOF_i^l \,||\, SIG_i^l$という形をしている。

【０７３５】

$DATA_i^{l-1}$はU_{l-1}から送られてきたメッセージ、$BODY_i^l$はメッセージの本体、$PROOF_i^l$は$BODY_i^l$の正当性証明文、SIG_i^lはU_lの$DATA_i^{l-1} \,||\, BODY_i^l \,||\, PROOF_i^l$に対する署名。

【０７３６】

１周目、２周目、３周目の計算の概略を説明する。

【０７３７】

第i周目の計算において、U_lはまず$DATA_i^{l-1}$をU_{l-1}から受け取る(1501)。

【０７３８】

(一周目のU_lのみは例外的に自分で作ったデータ$DATA_0^l$を使う)。

【０７３９】

$DATA_i^{l-1}$を受け取ったら、U_lは正当性証明文$PROOF_1^l$、…,$PROOF_{l-1}^l$を全て検証する(1502)。そして次にU_lは署名文SIG_1^l、…、SIG_{l-1}^lを全て検証する(1503)。

【０７４０】

第1周目の場合で、しかもl=1の場合のみ1504の計算を行う。次にU_lは乱数生成を行う(1505)。

そしてU_lはその乱数を用いて本計算を行い、$BODY_i^l$を作成する(1506)。本計算を終えたらU_lは$BODY_i^l$の正当性証明文$PROOF_i^l$を作成する(1507)。そしてU_lは$DATA_i^{l-1} \,||\, BODY_i^l \,||\, PROOF_i^l$に対する署名文$SIG_i^l$を作成する(1508)。

【０７４１】

最後にU_lは$DATA_i^l = DATA_i^{l-1} \,||\, BODY_i^l \,||\, PROOF_i^l \,||\, SIG_i^l$を$U_{l+1}$に送信する(1509)。

【０７４２】

[記号]

以下に、本明細書で使用する記号の説明を行う。

【０７４３】

[暗号方式E[27]]

G[1]を、アーベル群でDDH問題が難しいもの(例えば有限体上の楕円曲線群)とし、G[1]の位数をpとし、G[1]の零元をＯと表す。

【０７４４】

ηを記号とし、以下の記号を定義する。ただし、

【０７４５】

【数２８５】

$$P[|0|] \in G[1]$$

【０７４６】

に対し、(P[|0|],0)を略記して単にP[|0|]と表し、自然に

【０７４７】

【数２８６】

$$F_p \subset B[12],\ G[1] \subset G[12B]$$

【０７４８】
とみなし、G[12B]上の和を成分毎の和
により定義し、
【０７４９】
【数２８７】

$$W[12] = B12^{\kappa} \text{ とし、}$$
$$G[12W] = G[12B]^{\kappa} \text{ とする。}$$
$$w[2] \in W[12]$$

【０７５０】
のα成分をw[2|α|]と表し、W[12]上の和と積を成分毎の和と積により定義し、G[12W]上の和とスカラー倍を成分毎の和とスカラー倍により定義する。
【０７５１】
【数２８８】

- $B[12]=F_p[\eta]/(\eta^2-1)$,
- $\phi[24](1)=1$, $\phi[24](0)=\eta$,
- $G[12B]=G[1]^2$、
- aP[2]=(a[|0|]P[|0|]+a[|1|]P[|1|],aa[|0|]Pa[|1|]+a[|1|]Pa[|0|])
- $W[12]=B[12]^{\kappa}$、
- e[|i|]=(0,…,0,1,0,…,0)（i番目のみが1）
- $\phi[2]: F_p \rightarrow W[12]$を$x \rightarrow \Sigma_{\alpha}\ \phi[2](x[|\alpha|])e[|\alpha|]$
- ただしここで
  - P[2]=(P[|0|],P[|1|]), P[23]=(P[3|0|],P[3|1|]) ∈ G[12B], a=a[|0|]+a[|1|]η ∈ B[12]、P[2]=(P[|0|],P[|1|]) ∈ G[12B],
  - κ：pのビット数,
  - x=x[|k-1|] || … || x[|0|],
  - $G[12W]=G[12B]^{\kappa}$,

【０７５２】
暗号方式E[27]はG[12W]における、楕円ElGamal暗号の類似物である。
【０７５３】
秘密鍵空間をF_p、公開鍵空間を$G[12W]^2$、平文空間をG[12W]、乱数空間をW[12]とする。
【０７５４】
鍵生成をするには、P=P[|0|]+ηP[|1|]でP[|0|],P[|1|]≠０となるものを任意に選ぶ。ランダムに
【０７５５】

【数２８９】

$$a \in F_p$$

【０７５６】
を選び、Q=aPとする。aが秘密鍵、
(P,Q)が公開鍵である。
平文Mを暗号化するには一様かつランダムに
【０７５７】
【数２９０】

$$r \in B[12]$$

【０７５８】
を選び、
暗号文(P[3],Q[3])=(rP,M+rQ)を計算する。
(P[3],Q[3])を復号するにはQ[3]-aP[3]を計算すれば良い。
[暗号方式E[2],E[25]]
以下を定義する：
【０７５９】
【数２９１】

- K[1]={ {x[|wWh|]}(w∈C[1],W∈{L,R},h∈{0,1}を走る) | x[|wWh|]∈F
- A[12]={ { a[2|wWijk|]} ({w∈C[1],W∈{L,R},i,j,k∈{0,1}}を走る)|a[
- A[125]={ { A[25|wWijk|i[6]j[6]k[6]]({w∈C[1],W∈{L,R},i,i[6],j,j[
  |A[25|wWijk|i[6]j[6]k[6]]∈W[12]}
- G[1|K|]={ {P[|wWh|]} ({w∈C[1],W∈{L,R},h∈{0,1}} を走る)|P[|wWh
- G[12|A|]={{ P[2|wWijk|]}(w∈C[1],W∈{L,R},i,j,k∈{0,1}})|P[2|wWi
- G[124|A|]={ { P[24|wWijk|i[6]j[6]k[6]]}
({w∈C[1],W∈{L,R},i,j,k,i[6],j[6],k[6]∈{0,1}}を走る)
  |P[24|wWijk|i[6]j[6]k[6]]∈G[12W],
- aA=(aA[|1|],aA[|2|])
- a[5]A[5]=(a[5]A[5|1|],a[5]A[5|2|])
- ただしここで
  - a ∈A[12]
  - A=(a[|1|],A[|2|]) ∈ $G[12|A|]^2$
  - a[5] ∈ A[125]
  - A[5]=(A[5|1|],A[5|2|]) ∈ $G[124|A|]^2$

【０７６０】
κの元xのwWh成分をx[|wWh|]と書く事にし、
A[12]の元x[2]のwWijk成分をx[|wWijk|]と書く事にし、
A[125]の元A[25]のwWijk,i[6],j[6]｝,k[6]成分をx[|wWijk|i[6]j[6]k[6]]
と書く事にする。
【０７６１】
多重配列の和と積、スカラー倍を、成分毎の和と積により定義する。
ただし例外的に、A[125]の元同士の積、およびG[124|A|]の元のA[125]の元によるスカラ

一倍のみは

【０７６２】

【数２９２】

● a[25]*b[25]=Σ$_{i[7],j[7],k[7]}$
a[25|wWijk|i[7]j[7]k[7]]
b[25|wWi[7]j[7]k[7]|i[6]j[6]k[6]],

● a[25]*P[24]=Σ a[25|wWijk|i[7]j[7]k[7]]
P[24|wWi[7] j[7] k[7]|i[7]j[7]k[7]]
(i[7],j[7],k[7]に関する和)

【０７６３】

により定義する。

【０７６４】

以下の記号を定義する。

【０７６５】

【数２９３】

● E[25][(Z[2]|s[25])](M[25])
=
{E[27][(Z[2]|s[25|wWijk|i[6]j[6]k[6]])](M[25|wWijk|i[6]j[6]k[6]])}

● E[25][(Y[2]|s[25])](M[25])
=
E[25][(s[25]|Z[25])](M[25])

● E[2][(x[2]|r[2])](M[2])
=
{E[27][(x[2|wWijk|]|r[2|wWijk|])](M[2|wWijk|])

● E[2][(Y[2]|r[2])](M[2])
=
E[2][(x[2]|r[2])](M[2])

・ ただしここで

● M[25]={M[25|wWijk|i[6]j[6]k[6]]},
M[25|wWijk|i[6]j[6]k[6]] ∈ G[12W]
● Z[2]={Z[25|wWijk|i[6]j[6]k[6]]},
(Z[25|wWijk|i[6]j[6]k[6]] ∈ G[12W]^2)
● s[25]={s[25|wWijk|i[6]j[6]k[6]]}∈A[125]
● Y[2]=(P[2],r[2])∈G[12W],
● Z[25]={Y[2]}[|wWijk|i[6]j[6]k[6]]
● M[2]={M[2|wWijk|]}[|wWijk|] (M[2|wWijk|] ∈ G[12W])
● x[2]=(P[2],Q[2])=({P[2|wWijk|]},{ Q[2]
[|wWijk|]})
(P[2|wWijk|], Q[2|wWijk|]∈G[12W]),
● r[2]={r[2|wWijk|]}, r[2|wWijk|]∈{}W[12]

【０７６６】

暗号方式E[2]、E[25]をそれぞれ、真理値群環上の多重配列エルガマル暗号、真理値群環上の拡張多重配列エルガマル暗号と呼ぶ事にする。

［その他の記号］

【０７６７】

【数２９４】

- h[:l|w|](ijk))=(i□[|w|]j)○k
- F[25:l| λ[|1|], λ[|2|], λ[|2|]|](x[2])=
  {x[2:l|wh[|w|](ijk)|]
  δ(i,i[6]○λ[|1w|]),
  δ(j,j[6]○λ[|2w|]),
  δ(k,k[6]○λ[|3w|])}
  (wWij[6]jj[6]kk[6]に関する属)。
- J[2](x[2]) ∈ A[12]=J[2](x[2])={x[2|W(w)i[W]|]、
- π[2](a[25])={Σa[25|wWijk|i[6]j[6]k[6]]}[|ijk|]}
  (和はi[6]、j[6]、k[6]に関する和)

【０７６８】
ただしここで
【０７６９】
【数２９５】

- λ[|1|]={λ[|1w|]}、λ[|2|]={λ[|2w|]}、
λ[|3|]={λ[|3w|]}：ビットの属。(w∈C [1]に関する属)。
- x[2]={x[2|wWh|]} x[2|wWh|]∈ W[12],
- 「○」：ビット毎の排他的論理和。
- 「□[|w|]」：素子wで計算する演算子。
  (ただしwが入力素子の時はi□[|w|]j=1(if b_wをU_1, …,
  U_{l-1}のいずれかが持っている)、i□[|w|]j=0 (othewise)。)
- δ(i,i[6])：クロネッカーのデルタ。
- i[W]=i (if w=L), i[W]=j (if w=R),
- a[25]={a[25|wWijk|i[6]j[6]k[6]]} ∈ A[125]

【０７７０】
と定義する。
簡単な計算から、次が成立する事が分かる：
【０７７１】

【数２９６】

- (a[25]*b[25])c[25]=a[25]*(b[25]*c[25]),
- (a[25]*b[25])P[2]=a[25]*(b[25]{}P[2]),
- F[25:1|λ[3|1|],λ[3|2|],λ[3|3|]|](1)
  *F[25:1|λ[|1|],λ[|2|],λ[|3|]|](x[2])
  =
  F[25:1|λ[3|1|]○λ[|1|],λ[3|2|]○λ[|2|],λ[3|3|]○λ[|3|]|](x[2])
- F[25:1|λ[|1|],λ[|2|],λ[|3|]|](x[2])
  *F[25:1|0,0,0|](x[23])=F[25|λ[|1|],λ[|2|],λ[|3|]|](x[2]○x[23])
  ただしここで
  - a[25],b[25],c[25]∈A[125],
  - a[2],b[2]∈A[12],
  - x[2],x[23] ∈ κ,
  - λ[|1|]={λ[|1w|]},λ[|2|]={λ[|2w|]}
    λ[|3|]={λ[|3w|]},
    λ[3|1|]={λ[|1w|]}、
    λ[3|2|]={λ[|2w|]}、
    λ[3|3|]={λ[|3w|]}：ビットの配列
  - ｉ ∈ {1,…,N}

【０７７２】
[第0周目の計算の詳細]
第0周目の計算の詳細を述べる。
【０７７３】
U_1が$BODY_1{}^0$を計算する方法を説明する。
【０７７４】
U_1は以下を計算する。
【０７７５】

【数２９７】

- x[:0|wWh|]=0,
- x[2:0|wWh|]
  =
  ϕ[2](x[:0|wWh|]),
- x[:0]
  =
  {x[:0|wWh|]},
- x[2:0]
  =
  {x[2:0|wWh|]},
- λ[:0]={λ[:0|w|]={0},
  λ[L:0]={λ[:0|L(w)|]={0},
  λ[R:0]={λ[:0|R(w)|]={0},
- r[2:0]={r[2:0|wWijk|]}={0} （wWijkに関する属）
- y[:0]=0,
  r[2:0]=y[:0]P[2](=O), Y[2:0]=(P[2],r[2:0])
- s[2:0|S|]={(s[2:0|S|])[|wWijk|i[6]j[6]k[6]]}
  ={0}[|wWijk|i[6]j[6]k[6]],
- s[2:0|T|]={(s[2:0|T|])[|wWijk|i[6]j[6]k[6]]}
  ={0}[|wWijk|i[6]j[6]k[6]],
- s[25U:0]={(s[25U:0|wWijk|i[6]j[6]k[6]]}
  ={0}[|wWijk|i[6]j[6]k[6]],
- (S[2:0],T[2:0],U[25:0]) = (E[2][(Y[2:0]|s[2:0|S|])](r[2:0]P[2])
- E[2][(Y[2:0]|s[2:0|T|])](r[2:0]Q[2:0]),
- E[25][(Y[2:0]|s[25R:0])](F[25:||λ[L:0], λ[R:0], λ[:0]|](x[2:0])P[2])
- $BODY_1^0$ =
  (Q[2:0],r[2:0]) || (s[2:0],T[2:0],U[25:0]).
  ただしここで
  - w∈{}C[1],W∈ {L,R},h∈{0,1},i,j,k∈{0,1}

【０７７６】

[第1周目の計算の詳細]

一周目のマルチパーティ計算を説明する。図１５に則して説明する。

[データの取得1501の詳細]

各U_lはU_{l-1}からデータ$DATA_1^{l-1}$を受け取る。(U_1のみは、例外的に自分でデータ$DATA_1^{1-1}=DATA_1^0$を計算する)。

[データ中の証明文の検証1502の詳細]

さてU_{l-1}から$DATA_1^{l-1}$ || $BODY_1^{l-1}$ || $PROOF_1^{l-1}$ || SIG_1^{l-1} ||が送られてきたら、U_lは$PROOF_1^1$、…,$PROOF_1^{l-1}$の正当性を確認する。この正当性の確認についての詳細は後述する。

[データ中の署名文の検証1503の詳細]

U_lはSIG_1^1、…、 SIG_1^{l-1}の正当性を確認する。さらにRANDのハッシュ値Pを計算し、P[2]=(e[|0|]+…+e[|κ-1|])(1+η)Pを確認する。

[U_1のみ行う計算1504の詳細]

U_1はまず、乱数RANDを任意に選び、RANDのハッシュ値

【０７７７】

【数２９８】

$$P \in G[1]$$

【０７７８】
とし、P[2]=(e[|0|]+…+e[|κ-1|])P[2B]とし、$BODY_1^{-1}$= RAND || P[2]とし、そしてBODY$_1^0$を後で説明する手順に従って自分で作成し、さらに$PROOF_1^0=SIG_1^0=\varepsilon$とし、$DATA_1^0$=RAND||$BODY_1^0$||$PROOF_1^0$||$SIG_1^0$とする。
【０７７９】
[乱数生成1505の詳細]
U_lはランダムに以下を選ぶ(ただしかっこ内の記述を満たすように選ぶこと)：
【０７８０】
【数２９９】

- {x[#l|wh|]} (x[#l|w[t]0|]}=0,
  x[0#l|w[t]0|]=1,
  x[#l|wh|]∈K[l],各x[#l|wh|]の最上位ビットは1)。
- {x[|wWh|]},x[|wWh|] ∈{0,1} (x[#l|wLh|]○x[#l|wRh|]=x[#l|wh|])
{w∈C[1],W∈{L,R},h∈{0,1}}
- r[2]={r[2|wWijk|]}∈A[12],
- r[2|wWijk|]∈F_p^{κ}⊂B[12]$^{\kappa}$=W[12],
- s[2|S|]={(s[2|S|])[|wWijk|]}∈A[12],
- s[2|T|]={(s[2|T|])[|wWijk|]}∈A[12],
- s[25U]={s[25U|wWijk|i[6]j[6]k[6]]}∈A[125].
- λ[#l]={λ[#l|w|]} (ビットの属，λ[|w[t]|]=0)
- y[#l]∈ F_p⊂ κ

【０７８１】
●W_t：出力素子
入力素子wに対し、形式的にx[#1|L(w)0|]=x[#1|R(w)1|]=0と定義する。
【０７８２】
以下の記号を定義する。
【０７８３】

【数３００】

●
x[:I|wWh|]=○x[#γ|wWh|],（γ≦Iの範囲の排他的論理和を取る）。
x[:I]={x[:I|wWh|]},
x[2#I|wWh|]=φ[2](x[#I|wWh|]),
x[2#I]={x[2#I|wWh|]},
x[2:I|wWh|]=φ[2:I](x[|wWh|]),
x[2:I]={x[2:I|wWh|]},

●
λ[#I]={λ[#I|w|]},
λ[L#I]={λ[#I|L(w)|]},
λ[R#I]={λ[#I|R(w)|]},
λ[:I|w|]=Σλ[#γ|w|],（γ≦Iの範囲の和を取る）
λ[:I]={λ[:I|w|]},
λ[L:I]={λ[:I|L(w)|]},
λ[R:I]={λ[:I|R(w)|]},

● Y[2:I]=(P[2],y[:I]P[2]),
y[:I]=Σy[#I],（γ≦Iの範囲の和を取る）

【０７８４】
提案方式に関し、次の事実が言える。ユーザ達がプロトコルにしたがっている場合、各U_1の送るデータ$BODY_1^1$は以下を満たす。
● $BODY_1^1$ = (Q[2:1],r[2:1]) || (s[2:1],T[2:1],U[25:1])、
● (Q[2:1],r[2:1])=J[2](x[2:1])P[2],y[:1]P[2])、
● (s[2:1],T[2:1],U[25:1])=(E[2][(Y[2:1]|s[2][S:1])](r[2:1]P[2]),
E[2][(Y[2:1]|s[2:1|T|])](r[2:1]Q[2:1]),
E[25][(Y[2:1]|s[25U:1])](F[25:1|λ[L:1],λ[R:1],λ[:1]|](x[2:1])P[2])
ただしここで
【０７８５】
【数３０１】

● s[2:I|S|]
=
Σs[2#γ|S|]　（γ≦Iの範囲の和を取る），
● s[2:I|T|]
=
Σs[2#γ|T|],
●
s[25U:I]= [235U:I]+s[25U#I],
s[235U:I]
=
F[25:I|λ[L#I],λ[R#I],λ[#I]|](1)
* s[25U:I-1]
* F[25:I|0,0,0|](x[2#I]),

【０７８６】
[本計算1506の詳細]
一周目のマルチパーティ計算の本計算1506を図１７に則して説明する。
【０７８７】
U_1が$BODY_1^1$を計算する方法を説明する。

【０７８８】
[再暗号用の公開鍵の計算1701]
U_1はまず、
● Q[2:1]=J[2]x[2#1])Q[2:1-1]
● r[2:1]=y[#1]P[2]+r[2:1-1]
を計算する。
【０７８９】
[データの変換1702]
● S[23:1]=r[2#1]s[2:1-1]
● T[23:1]=r[2#1]J[2](x[2#1])T[2:1-1],
● U[235:1]=F[25:1|λ[L#1],λ[R#1],λ[#1]|](1)*U[25:1-1]*F[25:1|0,0,0|](x[2#1])
を計算する。
【０７９０】
なお、この時次が言える：
● Q[2:1]=J[2](x[2:1])P[2]、
● r[2:1]=y[:1]P[2]、
● S[23:1]=E[2][(Y[2:1-1]|s[2:1-1|S|])](r[2:1]P[2]),
● T[23:1]= E[2][(Y[2:1-1]|s[2:1-1|T|])](r[2:1]Q[2:1]),
● U[235:1]=E[25][(Y[2:1-1]|s[235U:1])](F[25:1|λ[L:1],λ[R:1],λ[:1]|](x[2:1])P[2])。
【０７９１】
ただしここで
●s[235U:1]=F[25:1|λ[L#1],λ[R#1],λ[#1]|](1)
*s[25U:1-1]
*F[25:1|0,0,0|](x[2#1])
[再暗号化-秘密鍵の変換1703、再暗号化-乱数の変換1704、正当性証明文の作成1507、署名文の作成1508、データの送信1509]
最後にU_1は以下を計算する。(かっこ内は図中の番号)。
●(1703)
s[233:1]=S[23:1|1|],S[23:1|2|]+y[#1]s[2:1|1|]),
・
T[233:1]=T[23:1|1|],T[23:1|2|]+y[#1]T[2:1|1|]),
・
T[2335:1]=(U[235:1|1|],U[235:1|2|]+y[#1]U[25:1|1|]),
●(1704)
s[2:1]=s[233:1]+E[2][(Y[2:1]|s[2#1|S|])](O),
T[2:1]=T[233:1]+E[2][(Y[2:1]|s[2#1|T|])](O)
U[235:1]=(U[235:1|1|],U[235:1|2|]),
U[25:1]=T[2335:1]+E[25][(Y[2:1]|s[25U#1])](O),
(s[2:1],T[2:1],U[25:1])
=
(E[2][(Y[2:1]|s[2:1|S|])](r[2:1]P[2]),
E[2][(Y[2:1]|s[2:1|T|])](r[2:1]Q[2:1]),
E[25][(Y[2:1]|s[25U:1])]
(F[25:1][(λ[L:1],λ[R:1],λ[:1]|)](x[2:1]P[2]),
●(1507)
●(1508)
・$BODY_1^1$=s[2:1]
・$DATA_1^{1-1}$ || $BODY_1^{1-1}$ || $PROOF_1^{1-1}$の署名
SIG_1^1を作成。

●(1509)
$DATA_1^{l}$
$=DATA_1^{l-1}$ || $BODY_1^{l}$ || $PROOF_1^{l}$ || SIG_1^{l}
$DATA_1^{l}$をU_{l+1}
ただしここで
● S[23:1]=E[2][(Y[2:1-1]|s[2:1-1|S|])](r[2:1]P[2]),
● T[23:1]=E[2][(Y[2:1-1]|s[2:1-1|T|])](r[2:1]P[2]),
● U[235:1]=E[25][(Y[2:1-1]|s[25U:1-1])](r[25:1]P[2]),
● S[23:1]=(S[23:1|1|],S[23:1|2|]),
● T[23:1]=(T[23:1|1|],T[23:1|2|]),
● T[23:1]=(T[23:1|1|],T[23:1|2|]),
正当性証明文の作成1507の詳細は長いので説明を後にまわす。
【０７９２】
$DATA_1^{l}$=(Q[2:1],r[2:1]) || (s[2:1],T[2:1],U[25:1])をU_{l+1}に送る。
【０７９３】
なお、この時次が言える：
●S[233:1] =E[2][(Y[2:1]|s[2:1-1|S|])](r[2:1]P[2])、
●s[2:1] = E[2][(Y[2:1]|s[2:1|S|])](r[2:1]P[2])。
[第2周目の計算の詳細]
第二周目の計算の詳細を図１５に則して説明する。
【０７９４】
[データの取得1501の詳細]
各U_lはU_{l-1}からデータ
$DATA_2^{l-1}$
=
$DATA_2^{l-2}$ || $BODY_2^{l-1}$ || $PROOF_2^{l-1}$ || SIG_2^{l-1}
を受け取る。
【０７９５】
[データ中の証明文の検証1502、データ中の署名文の検証1503、U_lのみ行う計算1504、乱数生成1505の詳細、F_p上の暗号の算出1801]
以下の計算を行う。
●(1502)$PROOF_2^{1}$ || … || $PROOF_2^{l-1}$の正当性検証(詳細は後述)。
●(1503)SIG_2^{1} || … || SIG_2^{l-1}の正当性検証
●(1504)何もしない
●(1505)何もしない
[本計算1506の詳細]
第二周目の計算の本計算1506の詳細を図１８に則して説明する。
【０７９６】
[F_p上の暗号の算出1801]
この節では以後添字「:N」を省略する。
【０７９７】
U_lは以下の計算をする：
●s[2U]=π[2](s[25U]),
●m[2S]= r[2],
●m[2T]= r[2]J[2](x[2]),
●m[2U]= F[25|λ[L],λ[R],λ|](x[2]),
●U[2]=π[2](U[25])
●(s[2],T[2],U[2])
=
E[2][(Y[2]|s[2|S|])](m[2S]P[2]),

E[2][(Y[2]|s[2|T|])](m[2T]P[2]),
E[2][(Y[2]|s[2U])](m[2U]P[2])
　ただしここで
●X={(P,x[|wh|]P)}、Y={(P,yP)},
●E[1][(r|X)](A)={E[7][(r[|wWijk|]|X)](A[|wWijk|]P)}
●E[7]：楕円ElGamal暗号方式の暗号化関数。
　【０７９８】
　さらに以下の計算をする。
　【０７９９】
　　【数３０２】

● (s[24V|wWijk|]=Σs[2V|αwWijk|],(αに関する和を取る)
● (m[24V|wWijk|]=Σ2αm[2V])[|αwWijk|],(αに関する和を取る)
● (s[24V|wWijk|]P[2B||]=Σ2αs[2V|αwWijk|]P[2]),(αに関する和を取る)
● s[24V]P[2B]=(s[4V|0,wWijk|]P,s[4V|1,wWijk|]P),
● (m[24V|wWijk|]+(s[24V|wWijk|]y)P[2B]
　　=
　　Σ2αm[2V|αwWijk|]+s[2V|αwWijk|])yP[2B](αに関する和を取る)
●
●
・ ただしここで

　　● (s[2V|wWijk|]
　　=
　　Σs[2V|αwWijk|]e[α] (αに関する和を取る)
● (s[24V|wWijk|]=((s[V|0,wWijk|],(s[V])[|1,wWijk|])
● (m[2V|wWijk|]=m[2V|wWijk|]
　　=
　　Σm[2Vα|wWijk|]e[|α|],(αに関する和を取る)
● m[24V|wWijk|]=(m[4V|0,wWijk|],m[4V|1,wWijk|]),
● P[2]
　　=
　　Σe[|α|]P[2B] (αに関する和を取る)
● P[2B]=(P,P), P∈{}G[1],
● V[2]
　　=
　　E[2][(Y[2]|s[2V])](r[2]P[2])
　　=
　　(s[2V]P[2],m[2V]P[2]+s[2V]r[2]),
● s[2V|wWijk|]P[2]
　　=
　　Σ(s[2Vα|wWijk|]e[|α|]P[2B], (αに関する和を取る)
● (m[2V|wWijk|]+s[2V|wWijk|]・y)P[2B] ∈ W[12]
　　=
　　Σ(((m[2V])[|α|])[|wWijk|]+s[2V|α||wWijk|]yP[2B]e[|α|]。
　　(αに関する和を取る)
● (m[24V|wWijk|]+s[24V|wWijk|]y)P[2B]
　　=
　　(m[4V|0,wWijk|]+s[V|0,wWijk|]y)P,
　　(m[4V|1,wWijk|]+s[V|0,wWijk|]y)P

【０８００】

よってU_lは以下を得る事ができる：
●s[V|0,wWijk|]P、s[V|1,wWijk|]P,
●m[4V|0,wWijk|]+s[V|0,wWijk|]y)P,
m[4V|1,wWijk|]+s[V|0,wWijk|]y)P,
さらに以下を計算する。
●R=yP、Y=(P,R)
●(s[V|0,wWijk|]P,
(m[4V|0,wWijk|]+s[V|0,wWijk|]y)P
=
E[(s[V|0,wWijk|]|Y)](m[4V|0,wWijk|]P),
●(S,T+U)
=
(E[3][(s[4S0],s[4T0]+s[4U0]|Y)],E[1][(r[40]|J(X))](F[|λ[L],λ[R],λ|](x))
●{(Θ[|wWijk|],Θ'[|wWijk|])}
=
E[3][(s[4S0],s[4T0]+s[4U0]|Y)],E[1][(r[40]|J(X))](F[|λ[L],λ[R],λ|](x))
●
Θ[&0]
=
{(Θ[|wWij0|],Θ'[|wWij0|])}
●R[&0]=R_0
ただしここで
●r[2]=R[|0|]+R[|1|]η
[Θ[&1]の計算1802,正当性証明文の作成1507の詳細,署名文の作成1508の詳細,データの送信1509の詳細]
さらに以下の計算を行う：
●(1802)
●Θ[&1]=Θ[&1-1]-(Θ[|0|][&1-1],Θ[|1|][&1-1]-y[&1]Θ[|0|][&1-1]),
●$BODY_2^1$=Θ[&1]。
【０８０１】
ただしここで
●$BODY_2^{1-1}$=Θ[&1-1],
●Θ[&1-1]=(Θ[&1-1][0],Θ[&1-1|1|])
●(1508)
●(1803)
●$BODY_2^1$ = s[2:1]
●SIG_2^1：
$DATA_2^{1-1}$ || $BODY_2^1$ || $PROOF_2^1$への署名
そして$DATA_2^1$=$DATA_2^{1-1}$ || $BODY_2^1$ || $PROOF_2^1$ || SIG_2^1をU_{l+1}に送信する(1509)。
【０８０２】
[第3周目の計算の詳細]
３周目の計算の詳細を図１５に則して説明する。
【０８０３】
U_{l-1}から
$DATA_3^{1-1}$
=$DATA_3^{1-2}$ || $BODY_3^1$ || $PROOF_3^1$ || SIG_3^1
が送られてきたら（1501）、まず$PROOF_3^1$、…、$PROOF_3^{1-1}$、SIG_3^1、…、SIG_3^{1-1}の正当性を確認する（1502,1503）。(1504),(1505)は第三周目の計算ではない。$BODY_3^1$=εとし(1506)、$PROOF_3^1$=εとし(1507)、そして$DATA_3^{1-1}$ || $BODY_3^1$ || $PROOF_3^1$に対する署名SIG_3^1を作成し(1508)、$DATA_3^1$=$DATA_3^{1-1}$ || $BODY_3^1$ || $PROOF_3^1$ || SIG_3^1とし、$DATA_3^1$をU_lに

送る(1509)。
【０８０４】
[C[1]({b[|w|]})を求める方法1405]
C[1]({b[|w|]})を求める方法を説明する。
【０８０５】
まず入力素子wに対してx[#1|L(w)0|]=x[#1|R(w)1|]=0であるので、{E[1][(|{X[|W(w)i[|W|]|]})]x[|wWh[3](ij0)|])}を全て解き、Xx[|wWh[3](ij0)|]=x[|wWμ[w]|]を求め、x[3|w|]=x[|wμ[w]|]=x[|wLμ[w]|]○{|x[|wRμ[w]|]を計算し、μ[w]=h[3](ij0)とする。
【０８０６】
さて、下からu-1段目までの各素子wに対して、x[|μ[|w|]|]が求まっているとする。
【０８０７】
以下の計算をしてu段目のx[|μ[|w|]|]を求める。
●E[1][(|X[|L(w)μ[|L(w)|]|])]
(x[|{wWh[3](μ[|L(w)|]j0)}|]),
E[1][(|X[|R(w)μ[|R(w)|]|])]
(x[|wWh[3](iμ[|R(w)0)|]|]) (i,j=0,1)
をx[|W(w)μ[|W(w)|]|]を使って解く。
●x[|wh[3]μ[|L(w)|]μ[|R(w)0|]|]
=○x[|wWh[3]μL(w)μ[|R(w)0|]|]
(Wに関する排他的論理和)
ただしここで
●h[3](ijk)=h[|w|]((i○λ[|L(w)|])(j○λ[|R(w)|])(k○λ[|w|]))
●μ[w]=b[|w|]○λ[|w|]とし、
●b[|w|]：素子wの出力
●x[3|w|]=x[|wμ[w]|]
最終的にx[|μ[|w[|t|]|]|]=μ[|[|w[|t|]|]|]=b[|[|w[|t|]|]|]=C[1]({b[|w|]})を出力。
【０８０８】
[一周目の計算の正当性証明]
[一周目の計算の正当性証明の作成1507の詳細]
以下の記号を定義する：
【０８０９】
【数３０３】

- A[12|F_p|]={{a[2|wWijk|]}|a[2|wWijk|]∈F_p}、
- F[25:||a[|0|]b[|0|]c[|0|]|a[|1|]b[|1|]c[|1|]](u[2])∈A[12]を
  F[25:||abc|a[|6|]b[|6|]c[|6|]](u[2])
  =
  {x[2|h[:||wa[|i○i[6]|]b[|j○j[6]|]c[|k○k[6]|]|]|]|](ijk)}
- ただしここで
  - w：素子
  - z[2]∈K[12],
  - a[2]∈A[12],
  - a[25]∈A[125],
  - a[|0|],a[|1|],b[|0|],b[|1|],c[|0|],c[|1|],∈ F_p,
  - u[2]∈K[12],

【０８１０】

この節では、簡単の為添字「:1-1」を省略する。
【０８１１】
以下の方法で知識を証明する。
【０８１２】
まず乱数をハッシュ関数にいれて
【０８１３】
【数３０４】

$$P[6]\in G[1]$$

【０８１４】
を作る。そして以下を計算する。
●$P[26B]=(1+\eta)P$,
●$P[26]=\Sigma P[26B]e[|\alpha|]$、（$\alpha$に関する和を取る）
●$NOT(\lambda)=\{NOT(\lambda[|w|])\}$
U_1は以下の手順で$PROOF_1{}^1$を作成する。
ランダムかつ一様に以下のデータを選ぶ。
【０８１５】
【数３０５】

$$x[26\#1]\in\alpha,$$

$$\rho[26\#1|S[23]|]\in A[12]^2,$$

$$\rho[26\#1|S[233]||2|]\in A[12],$$

$$\rho[26T[2\&1]\#1]\in A[12]^2,$$

$$\rho[26T[233]\#1]\in A[12]^2,$$

$$\rho[26T[233]\#1|2|]\in A[12],$$

$$\rho[246\#1|T[233]||2|]\in A[12]^2,$$

$$\rho[256\#1|U[25\&1]|]\in A[125]^2,$$

$$\rho[256\#1|\lambda|]\in A[125],$$

$$\rho[256\#1|U[25\&2]|]\in A[125],$$

$$\rho[256\#1|U[25\&3]|]\in A[125],$$

$$\rho[256\#1|U[235:1]|]\in A[125]$$

$$\rho[256\#1|T[2335:1]||2|]\in A[12].$$

【０８１６】
そして以下を計算する。
●$C[2x[2]\#1|[|\alpha wWh|]|]=x[2\#1|\alpha wWh|]P[2B]+(x[26\#1|\alpha wWh|]P[26B]$,
$C[2x[2]\#1]=\{\Sigma e[|\alpha|]C[2x[2]\#1|[|\alpha wWh|]|]\}[|wWh|]$、（$\alpha$に関する和を取る）

●C[2#1|S[23]|] = S[23:1] +ρ[26S[23]#1]P[26],
τ[S[23]#1]=ρ[26S[23]#1],
●C[2S[23]#1]=(C[2S[23]#1|1|],(C[2S[23]#1])[|2|])を(C[2S[23]#1|1|],C[2S[23]#1|2|])と書く。
C[y,C[2S[23]]#1|1|]
=
yC[2S[23]#1|1|] +ρ[26S[233]#1|2|]P[26||]{A[12]},
C[2S[233]#1]=(C[2S[23]#1|1|],C[2S[233]#1|2|]),
C[2S[233]#1|2|]=C[2S[23]#1|2|]+C[2y,C[2S[23]]#1|1|],
τ[S[233]#1]=(τ[S[23]#1|1|],
τ[S[23]#1|2|]+yτ[S[23]#1|1|]+ρ[26S[233]#1])。
【０８１７】
ただしここで
(τ[S[23]#1|1|]、τ[S[23]#1|2|]) =(τ[S[23]#1])。
●C[2T[2&1]#1]=T[2&1:1]+ρ[26T[2&1]#1]P[26]を,
τ[T[2&1]#1] = ρ[26T[2&1]#1],
●C[2T[233]#1]=T[233:1] +ρ[26T[233]#1]P[26],
τ[T[233]#1]=ρ[26T[233]#1],
●C[2T[23:1]#1]=(C[2T[23:1]#1|1|],C[2T[23:1]#1|2|])を
(C[2T[23:1]#1|1|],C[2T[23:1]#1|2|])と書く。
C[y,C[2T[23:1]]#1|1|]=yC[2T[23:1]#1|1|] +ρ[26T[233]#1|2|]P[26A[12]],
C[2T[233]#1]=(C[2T[23:1]#1|1|],C[2T[233]#1|2|]),
C[2T[233]#1|2|]=C[2T[23:1]#1|2|]+C[2y,C[2T[23:1]]#1|1|],
τ[T[233]#1]=(τ[T[23:1]#1|1|],
τ[T[23:1]#1|2|]+yτ[T[23:1]#1|1|]+ρ[26T[233]#1])。
【０８１８】
ただしここで
(τ[T[23:1]#1|1|]、τ[T[23:1]#1|2|]) =τ[T[23:1]#1]。
●K[2y,C[2T[233]]#1|1|]=y[4#1]C[2T[23:1]]+ρ[246T[233]#1|1|]P[26],
●c[25U[25&1]#1]=U[25&1:1]+ρ[256#1|U[25&1]|]P[26],
τ[U[25&1]#1]=ρ[256#1|U[25&1]|]。
●C[2λ#1]=λ[#1]P[2]+ρ[256#1|λ|]P,
●ρ[256NOT(λ)#1]=-ρ[256λ#1],
C[2NOT(λ)#1]=P[2]-C[2λ#1],
●C[2U[25&2]#1]=F[25:1|λ[L]{}00|NOT(λ)[L]00](u[2])
C[2U[25&1]#1]+ρ[256#1|U[25&2]|]P[26],
ただしここで
NOT(λ)[L]={NOT(λ)[|L(w)|]}。
τ[U[25&2]#1]=F[25:1|λ[L]{}00|NOT(λ)[L]00](u[2])
τ[U[25&1]#1]+ρ[256#1|U[25&2]|],
●C[2U[25&3]#1]=F[25:1|0λ[R]0|0NOT(λ)[R]0](u[2])
C[2U[25&2]#1]+ρ[256U[25&3]#1]P[26],
ただしここで
NOT(λ)[R]={NOT(λ)[R|R(w)|]}。
τ[U[25&3]#1]=F[25:1|0λ[R]0|0NOT(λ)[R]0](u[2])
τ[U[25&2]#1]+ρ[256U[25&3]#1]。
●C[2U[235:1]#1]=F[25:1|00λ|00NOT(λ)](u[2])
C[2U[25&3]#1],
τ[U[235:1]#1]=F[25:1|00λ|00NOT(λ)](u[2])
τ[U[25&3]#1],

●C[2U[235:1]#1]=((C[2U[235:1]#1])[|1|],(C[2U[235:1]#1])[|2|])を(C[2U[235:1]#1|1|],C[2U[235:1]#1|2|])と書く。
C[y,C[2U[235:1]]#1|1|]=yC[2U[235:1]#1|1|] +ρ[256#1|T[2335:1]||2|]P[26A[12]],
C[2T[2335:1]#1]=(C[2U[235:1]#1|1|],C[2T[2335:1]#1|2|]),
C[2T[2335:1]#1|2|]=C[2U[235:1]#1|2|] +C[2y,C[2U[235:1]]#1|1|],
τ[T[2335:1]#1]=(τ[U[235:1]#1|1|],
τ[U[235:1]#1|2|]+yτ[U[235:1]#1|1|]+ρ[256T[2335:1]#1]),
ただしここで
(τ[U[235:1]#1|1|]、τ[U[235:1]#1|2|]) =τ[U[235:1]#1]。

【０８１９】
さらに以下の計算をする。

【０８２０】
【数３０６】

● x[2|αwWh|]P[2B]=1の時。

●
各αwWhに対し、
まずランダムにx[246&1|αwWh|]∈B[1]を選び、K[2&1|αwWh|]=
x[246&1|αwWh|]P[26B]
を計算。

● ランダムに
x[29&η|αwWh|],
c[2&η|αwWh|]∈B[1]を選び、
K[2&η|αwWh|]
=
x[29&η|αwWh|]P[26]
−c[2&η|αwWh|](C[2x[2]|αwWh|]−ηP[2B])を
計算する。

【０８２１】
●x[2|αwWh|]P[2B]=ηの時。

【０８２２】
【数３０７】

●
各αwWhに対し、
まずランダムにx[246&η|αwWh|]∈B[1]を選び、K[2&η|αwWh|]=
x[246&η|αwWh|]P[26B]を計算する。

● ランダムに
x[29&1|αwWh|], c[2&1|αwWh|]
∈B[1]を選び、
K[2&1|αwWh|]=x[29&1|αwWh|]P[26]
−c[2&1|αwWh|](C[2x[2]|αwWh|]−P[2B])を
計算し、
(K[2&1|αwWh|],
(K[2&η|αwWh|]を計算する。

【０８２３】
さらに以下のデータを一様かつランダムに選ぶ。
【０８２４】
【数３０８】

$$x[24\#I],\ x[246\#I] \in A[12],$$

$$y[4\#I] \in F_p,$$

$$r[24\#I] \in A[12F_p],$$
$$\rho[246S[23]\#I] \in A[12]^2,$$

$$\rho[246S[233]\#I|2|] \in A[12]^2,$$

$$s[24S\#I] \in A[125],\ \tau[4S[233]\#I] \in A[125]^2,$$

$$r[24\#I] \in A[12F_p],$$
$$\rho[246T[2\&1]\#I] \in A[12]^2,$$

$$\rho[246T[233]\#I] \in A[12]^2,$$

$$s[24T\#I] \in A[125],\ \tau[4T[233]\#I] \in A[125]^2,$$

$$\rho[2456U[25\&1]\#I] \in A[125]^2,$$

$$\rho[2456\lambda\#I] \in A[125],$$
$$\lambda[4\#I] \in F_p,$$

$$NOT(\lambda)[4\#I],$$
$$=$$
$$\{NOT(\lambda)[4\#I|w|]\},$$
$$NOT(\lambda)[\#I|w|] \in F_p,$$
$$\rho[2456U[25\&2]\#I] \in A[125],$$

$$\rho[2456T[2335:I]\#I|2|] \in A[12]^2,$$

$$s[245U\#I] \in A[125],\ \tau[4T[2335:I]\#I] \in A[125]^2,$$

【０８２５】
そして以下を計算する。
●$K[2x[2]\#1]=x[24\#1]P[2]+x[246\#1]P[26]$,
●$K[2J[2](x),Q[2]\#1]=J[2](x[24])Q[2]$,
【０８２６】

【数３０９】

$$K[2y\#1]a=y[4\#1]P\in F_p\subset B[1],$$

【０８２７】

●K[2r[2],s[2]#1]=r[24#1]s[2]+ρ[246S[23]#1]P[26],
●K[2y,C[2S[233]]#1|1|]=y[4#1]C[2S[23]]+ρ[246S[233]#1|1|]P[26],
●K[2s[24S]#1]=s[24S#1]Y[2]-τ[4S[233]#1]P[26],
●K[2r[2],T[2]#1]=r[24#1]T[2]+ρ[246T[2&1]#1]P[26],
●K[2J[2](x[2]),T[2&1]#1]=J[2](x[24#1])T[2&1]+ρ[246T[233]#1]P[26],
●K[2s[24T]#1]=s[24T#1]Y[2]-τ[4T[233]#1]P[26],
●K[25U[25&1]#1] =U[25:1-1]*F[25:1|0,0,0|](x[24#1])+ρ[2456U[25&1]#1]P[26],
●K[2λ,P[2]#1]=λ[4#1]P[2]+ρ[2456λ#1]P[26],
K[2λ,C[2λ]#1]=λ[4#1]C[2λ#1]+ρ[2456λ#1]P[26],
●λ[4L#1]={λ[4#1|L(w)|]},
NOT(λ)[4L#1]={NOT(λ)[4#1|L(w)|]},
K[2U[25&2]#1]=F[25:1|λ[4L]00|NOT(λ)[4L]00](1)*U[25&1]+ρ[2456U[25&2]#1]P[26],
●λ[4R#1]={λ[4#1|R(w)|]},
NOT(λ)[4R#1]={NOT(λ)[4R(w)#1]},
K[2U[25&3]#1]=F[25:1|0λ[4R]0|0NOT(λ)[4R]0](1)*U[25&2]+ρ[2456U[25&3]#1]P[26],
●λ[4R#1]={λ[4R(w)#1]},
NOT(λ)[4R#1]={NOT(λ)[4R(w)#1]},
K[2U[235:1]#1]=F[25:1|00λ[4]|00NOT(λ)[4]](1)*U[25&3],
●K[2y,C[2T[2335:1]]#1|1|]=y[4#1]C[2U[235:1]]+ρ[2456T[2335:1]#1|1|]P[26],
●K[2s[245U]#1]=s[245U#1]Y[2]-τ[4T[2335:1]#1]P[26],

さらに以下を計算する。

【０８２８】

さらに
c[#1]=
Hash(
$DATA_1^{1-1}$,
$BODY_1^{1}$,
C[2x[2]#1],
C[2S[23]#1],
(C[2S[23]#1|1|],C[2S[23]#1|2|]),
C[y,C[2S[23]]#1|1|],
C[2T[2&1]#1],
C[2T[233]#1],
(C[2T[23:1]#1|1|],C[2T[23:1]#1|2|]),
C[2T[233]#1],
K[2s[24T]#1]=s[24T#1]Y[2]
c[25U[25&1]#1],
C[2λ#1],
C[2NOT(λ)#1],
C[2U[25&2]#1],
C[2U[25&3]#1],
C[2U[235:1]#1],
(C[2U[235:1]#1|1|],C[2U[235:1]#1|2|]),
C[y,C[2U[235:1]]#1|1|],
C[2T[2335:1]#1|2|],

K[2&1|αwWh|],
K[2&η|αwWh|],
K[2x[2]#1],
K[2J[2](x),Q[2]#1],
K[2y#1],
K[2r[2],s[2]#1],
K[2y,C[2S[233]]#1|1|],
K[2s[24S]#1],
K[2r[2],T[2]#1],
K[2J[2](x[2]),T[2&1]#1],
K[25U[25&1]#1],
K[2λ,P[2]#1],
K[2λ,C[2λ]#1],
K[2U[25&2]#1],
K[2U[25&3]#1],
K[2U[235:1]#1],
K[2y,C[2T[2335:1]]#1|1|],
K[2s[245U]#1],
)
を計算する。

【０８２９】

ただしここでHashは、F_p値ハッシュ関数。

【０８３０】

そして次を計算。

●x[2|αwWh|]P[2B]=1の時。

●各αwWhに対し、c[2&1|αwWh|]=c[#1]-c[2&η|αwWh|]とし、
x[29&1|αwWh|]=c[2&1|αwWh|](x[26|α|])[|wWh|]+x[246&1|αwWh|]を計算。

●x[2|αwWh|]P[2B]=ηの時。

●各αwWhに対し、c[2&η|αwWh|]=c[#1]-c[2&1|αwWh|]とし、
x[29&η|αwWh|]=c[2&η|αwWh|](x[26|α|])[|wWh|]+x[246&η|αwWh|]を計算(c[#1]c[2&1|αwWh|],x[29&1|αwWh|]),c[2&η|αwWh|] ,x[29&η|αwWh|]))する。

【０８３１】

さらに次を計算。

●x[28#1]=c[#1]x[2#1]+x[24#1] ,
x[268#1]=c[#1]x[26#1]+x[246#1],
●y[8#1]=c[#1]y[#1]+y[4#1],
●r[28#1]=c[#1]r[2#1]+r[24#1],
ρ[268S[23]#1]=c[#1]ρ[26S[23]#1]+ρ[246S[23]#1],
●r[8#1]=c[#1]r[2#1]+r[24#1],
ρ[268S[233]#1|2|]=c[#1]ρ[26#1|S[233]||2|]+ρ[246S[233]#1|2|],
●s[28S#1]=c[#1]s[24S#1]+s[24S#1]、
τ[8S[233]#1]=c[#1]τ[S[233]#1]+τ[4S[233]#1],
●r[28#1]=c[#1]r[2#1]+r[24#1],
ρ[268T[2&1]#1]=c[#1]ρ[26T[2&1]#1]+ρ[246T[2&1]#1],
●ρ[268T[233]#1]=c[#1]ρ[26T[233]#1]+ρ[246T[233]#1],
●r[8#1]=c[#1]r[2#1]+r[24#1],
ρ[268T[233]#1|2|]=c[#1]ρ[26T[233]#1|2|]+ρ[246#1|T[233]||2|],
●s[28T#1]=c[#1]s[24T#1]+s[24T#1]、
τ[8T[233]#1]=c[#1]τ[T[233]#1]+τ[4T[233]#1],
●ρ[2568U[25&1]#1]=c[#1]ρ[256U[25&1]#1]+ρ[2456U[25&1]#1],

●λ[8#1]=c[#1]λ[#1]+λ[4#1],
ρ[2568λ#1]=c[#1]ρ[256λ#1]+ρ[2456λ#1],
●NOT(λ)[8#1]=c[#1]NOT(λ)[#1]+NOT(λ)[4#1]、
ρ[2568U[25&2]#1]=c[#1]ρ[256U[25&2]#1]+ρ[2456U[25&2]#1]P[26],
●ρ[2568U[25&3]#1]=c[#1]ρ[256U[25&3]#1]+ρ[2456U[25&3]#1]P[26],
●r[8#1]=c[#1]r[2#1]+r[24#1],
ρ[2568T[2335:1]#1|2|]=c[#1]ρ[256T[2335:1]#1|2|]+ρ[2456T[2335:1]#1|2|],
●s[258U#1]=c[#1]s[245U#1]+s[245U#1]、
τ[8T[2335:1]#1]=c[#1]τ[T[2335:1]#1]+τ[4T[2335:1]#1]。

【０８３２】

そして、

PROOF$_1$[1]=(
C[2x[2]#1],
C[2S[23]#1],
(C[2S[23]#1|1|],C[2S[23]#1|2|]),
C[y,C[2S[23]]#1|1|],
C[2T[2&1]#1],
C[2T[233]#1],
(C[2T[23:1]#1|1|],C[2T[23:1]#1|2|]),
C[2T[233]#1],
c[25U[25&1]#1],
C[2λ#1],
C[2NOT(λ)#1],
C[2U[25&2]#1],
C[2U[25&3]#1],
C[2U[235:1]#1],
(C[2U[235:1]#1|1|],C[2U[235:1]#1|2|]),
C[y,C[2U[235:1]]#1|1|],
C[2T[2335:1]#1|2|],
K[2&1|αwWh|],
K[2&η|αwWh|],
K[2x[2]#1],
K[2J[2](x),Q[2]#1],
K[2y#1],
K[2r[2],s[2]#1],
K[2y,C[2S[233]]#1|1|],
K[2s[24S]#1],
K[2r[2],T[2]#1],
K[2J[2](x[2]),T[2&1]#1],
K[2s[24T]#1],
K[25U[25&1]#1],
K[2λ,P[2]#1],
K[2λ,C[2λ]#1],
K[2U[25&2]#1],
K[2U[25&3]#1],
K[2U[235:1]#1],
K[2y,C[2T[2335:1]]#1|1|],
K[2s[245U]#1],
c[#1],
x[29&1|αwWh|]),

x[29&η|αwWh|])),
x[28#1] ,x[268#1],
y[8#1],
r[28#1],
ρ[268S[23]#1]
r[8#1]
ρ[268S[233]#1|2|]
s[28S#1]
r[28#1]
ρ[268T[2&1]#1]
ρ[268T[233]#1]
r[8#1]
ρ[268T[233]#1|2|]
ρ[2568U[25&1]#1],
λ[8#1] ,
ρ[2568λ#1] ,
NOT(λ)[8#1],
ρ[2568U[25&2]#1],
ρ[2568U[25&3]#1],
r[8#1]
ρ[2568T[2335:1]#1|2|]
s[258U#1]
)
とする。

【０８３３】

[一周目の計算の正当性証明の検証1502の詳細]

$PROOF_1^1$を受け取ったら、U_{l+1}は以下を確認する。

● c[#1]=
Hash(
$DATA_1^{l-1}$,
$BODY_1^1$,
C[2x[2]#1],
C[2S[23]#1],
(C[2S[23]#1|1|],C[2S[23]#1|2|]),
C[y,C[2S[23]]#1|1|],
C[2T[2&1]#1],
C[2T[233]#1],
(C[2T[23:1]#1|1|],C[2T[23:1]#1|2|]),
C[2T[233]#1],
K[2s[24T]#1]
c[25U[25&1]#1],
C[2λ#1],
C[2NOT(λ)#1],
C[2U[25&2]#1],
C[2U[25&3]#1],
C[2U[235:1]#1],
(C[2U[235:1]#1|1|],C[2U[235:1]#1|2|]),
C[y,C[2U[235:1]]#1|1|],
C[2T[2335:1]#1|2|],
K[2&1|αwWh|],

K[2&η|αwWh|],
K[2x[2]#1],
K[2J[2](x),Q[2]#1],
K[2y#1],
K[2r[2],s[2]#1],
K[2y,C[2S[233]]#1|1|],
K[2s[24S]#1],
K[2r[2],T[2]#1],
K[2J[2](x[2]),T[2&1]#1],
K[25U[25&1]#1],
K[2λ,P[2]#1],
K[2λ,C[2λ]#1],
K[2U[25&2]#1],
K[2U[25&3]#1],
K[2U[235:1]#1],
K[2y,C[2T[2335:1]]#1|1|],
K[2s[245U]#1],
),
●各αwWhに対し、以下が成立する事。
●c[#1]=c[2&1|αwWh|]+c[2&η|αwWh|]，
x[29&1|αwWh|] P[6B] =c[2&1|αwWh|]
(C[2x[2]|αwWh|]-P[2B])+K[2&1|αwWh|],
x[29&1|αwWh|] P[6B] =c[2&η|αwWh|]
(C[2x[2]|αwWh|]-ηP[2B])+K[2&η|αwWh|]
●以下が成立する事
【０８３４】

【数３１０】

x[28#I]P[2]+x[28#I]P[26] =
c[#I]C[2x[2]#I]+K[2x[2]#I],

J[2](x[28#I])Q[2#I] = J[2](c[#I])Q[2#I]+K[2J[2](x),Q[2]#I],

y[8#I] ∈ F_p,
y[8#I]P[2] = c[#I](r[2:I]-r[2]) +K[2y#I],

y[8#I] ∈ F_p,

r[28#I]s[2:I-1]
+
ρ[268S[23]#I]P[26]
=
c[#I]C[2S[23]#1] + K[2r[2],s[2]#I],

c[#I]C[2y,C[2S[23]]#I|1|]
+
K[2y,C[2S[23]]#I|1|]
=
y[8#I]C[2S[23]#I|2|]
+
ρ[268S[233]#I|2|]P[26A[12]],

c[#I](s[2#I]-C[2S[233]#I])
+
K[2s[24S]#I]
=
s[28S#I]Y[:I]
-
τ[8S[233]#I]P[2],

r[28#I]T[2:I-1]
+
ρ[268T[2&1]#I]P[26]
=
c[#I]C[2T[2&1]#I] + K[2r[2],T[2]#I],

J[2](x[28#I])T[2&1:I-1]
+
ρ[268T[233]#I]P[26]
=
c[#I]C[2T[233]#I] + K[2r[2],T[2&1]#I],

c[#I]C[2y,C[2T[23:I]]#I|1|]
+
K[2y,C[2T[23:I]]#I|1|]
=
y[8#I]C[2T[23:I]#I|2|]
+
ρ[268T[233]#I|2|]P[26A[12]],

【０８３５】
を確認する。
【０８３６】

【数３１１】

●

c[#I](T[2#I]-C[2T[233]#I])
+
K[2s[24T]#I]
=
s[28T#I]Y[:I]
−
τ[8T[233]#I]P[2],

●

r[28#I]∈A[12F_p],

●

U[25:I-1]*F[25:I|0,0,0|](x[28#I])
+
ρ[2568U[25&1]#I]P[26]
=
c[#I]c[25U[25&1]#I]
+
K[25U[25&1]#I],

●

各wWijk,i[6],j[6],k[6]に対し
λ[8#I|wWijk|i[6],j[6],k[6]]∈ F_pとなる事、

【０８３７】
λ[8#1]P[2]+ρ[2568λ#1]P[26]=c[#1]C[2λ#1]+K[2λ,P[2]#1],
λ[8#1]C[2λ#1]+ρ[2568λ#1]P[26]=c[#1]C[2λ#1]+K[2λ,C[2λ]#1],
●C[2NOT(λ)#1]=P[2]-C[2λ#1],
●c[#1]C[2U[25&2]#1]+K[2U[25&2]#1]=F[25:1|λ[8L]00|NOT(λ)[8L]00](1)*U[25&1]+ρ[2568U[25&2]#1]P[26],
●c[#1]C[2U[25&3]#1]+K[2U[25&3]#1]=F[25:1|λ[8R]00|NOT(λ)[8R]00](1)*U[25&2]+ρ[2568U[25&3]#1]P[26],
●c[#1]C[2U[235:1]#1]+K[2U[235:1]#1]=F[25:1|{00λ[8]|00NOT(λ)[8]](1)*U[25&3],
●c[#1]C[2y,C[2U[235:1]]#1|1|]+K[2y,C[2U[235:1]]#1|1|]=y[8#1]C[2U[235:1]#1|2|]+ρ[2568T[2335:1]#1|2|]P[26A[12]],
●c[#1](U[2#1]-C[2T[2335:1]#1])+K[2s[245U]#1]=s[258U#1]Y[:1]-τ[8T[2335:1]#1]P[2]。

【０８３８】
[二周目の計算の正当性証明]
[二周目の計算の正当性証明の作成1507の詳細]
U_1はランダムに
【０８３９】
【数３１２】

$$y[4\&I] \in F_p$$

【０８４０】
を選び、
以下のようにして$PROOF_2{}^1$を計算する。

●P[4&l]=y[4&l]P,
Θ[4&l|1|]=y[4&l]Θ[&l|1|],
●c[&l]=Hash(DATA$_2^{l-1}$ || BODY$_2^{l-1}$
|| P[4&l] || Θ[4&l]),
● y[8&l]=c[&l]y[&l]+y[4&l],
●PROOF$_2^{l}$=P[4&l] || Θ[4&l]|| c[&l] || y[8&l]。

【０８４１】

[二周目の計算の正当性証明の検証1502の詳細]

PROOF$_1^{l}$を受け取ったら、U$_{l+1}$は以下を確認する。

● y[8&l]P=c(R[:l]-R[:l-1]})+P[4]
●y[8&l]Θ[8&l-1|0|]=c(Θ[&l-1|0|]-Θ[&l|0|])+Θ[4&l-1|0|]

【産業上の利用可能性】

【０８４２】

電子入札、電子競売等で、落札者以外の入札者の入札値を秘密にしたまま、入札者と入札価格を決定したい場合で、かつその決定が正しく行われたことを第三者が検証できる必要がある場合等や、電子投票等で匿名性を保ったまま正しく票数が数えられていることを第三者が検証できる必要がある場合等に、本発明方法を用いると有効である。

【０８４３】

なぜならば、本発明方法を用いれば、上記入札、競売、投票の結果を複数の計算装置で行えば、誰も計算結果以外の情報を新たに得ることがなく、かつその計算の正当性を誰でも検証できるからである。そしてこの計算が従来の技術を持ってして行うより効率的である。さらに、計算装置間の通信回数が少ないため、計算装置が通信に回線を確保するのに時間を費やす時間も少なく、効率的である。

【図面の簡単な説明】

【０８４４】

【図１】非特許文献1の従来の技術を説明したフローチャートである。

【図２】非特許文献1の従来の技術における、ガーブルド回路並列構築処理における、計算フェーズと通信フェーズの関係を示した図である．同じ番号が振られた計算装置が複数回記述されているが、これらは同一のもので、動作する時間が異なっているだけである．本図において、時は上から下へ流れるよう記述されている。

【図３】非特許文献2の従来の技術を説明したフローチャートである。

【図４】非特許文献2の従来の技術を説明したフローチャート「図(3)」における並列したランク判定処理の中で、並列して多数回行われる処理を一つだけ取り出して記述したフローチャートである。

【図５】本明細書提案の技術が従来方法の問題を解決するために考案した計算処理の流れを示すブロック図である。

【図６】第1の発明を実施するための最良の形態の動作の具体例を示すフローチャートである。

【図７】第1の発明を実施するための最良の形態の動作の具体例における、ElGamal暗号文準備処理の詳細を示すフローチャートの前半である。

【図８】第1の発明を実施するための最良の形態の動作の具体例における、ElGamal暗号文準備処理の詳細を示すフローチャートの後半である。

【図９】第1の発明を実施するための最良の形態の動作の具体例における、逐次置換再暗号処理の詳細を示すフローチャートの前半である。右の吹き出しの中に示されたフローチャートの処理を、各計算装置が順番に行う。

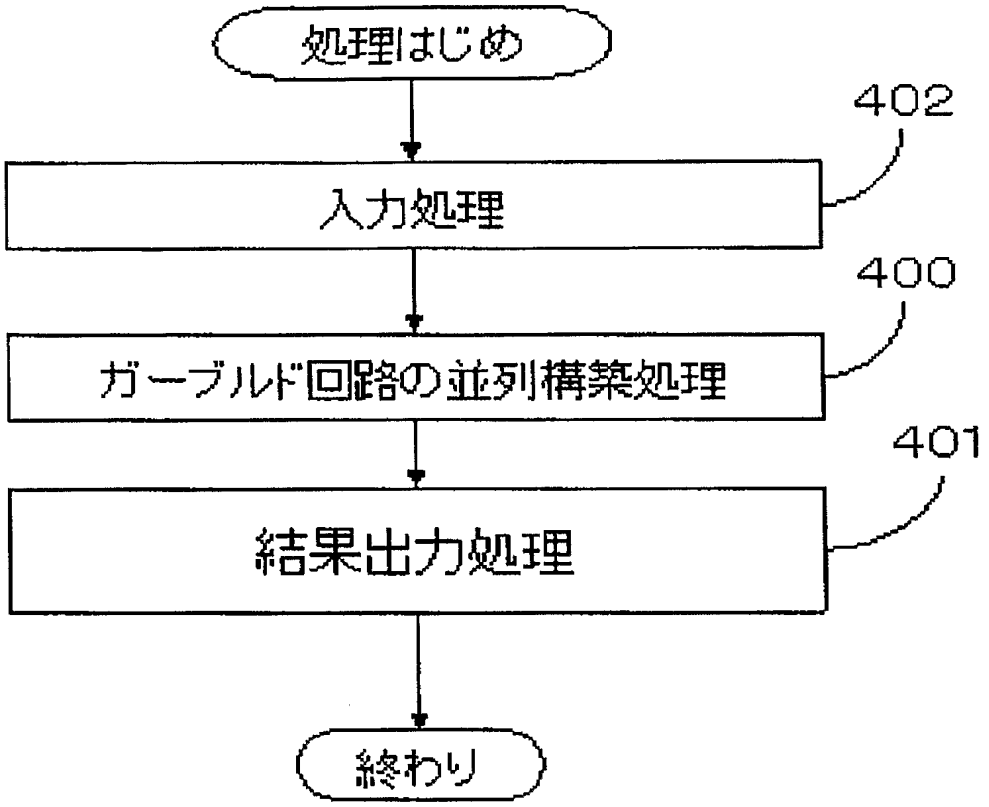
【図１０】第1の発明を実施するための最良の形態の動作の具体例における、結果出力処理の詳細を示すフローチャートである。

【図１１】第1の発明を実施するための最良の形態の構成を示すブロック図である。

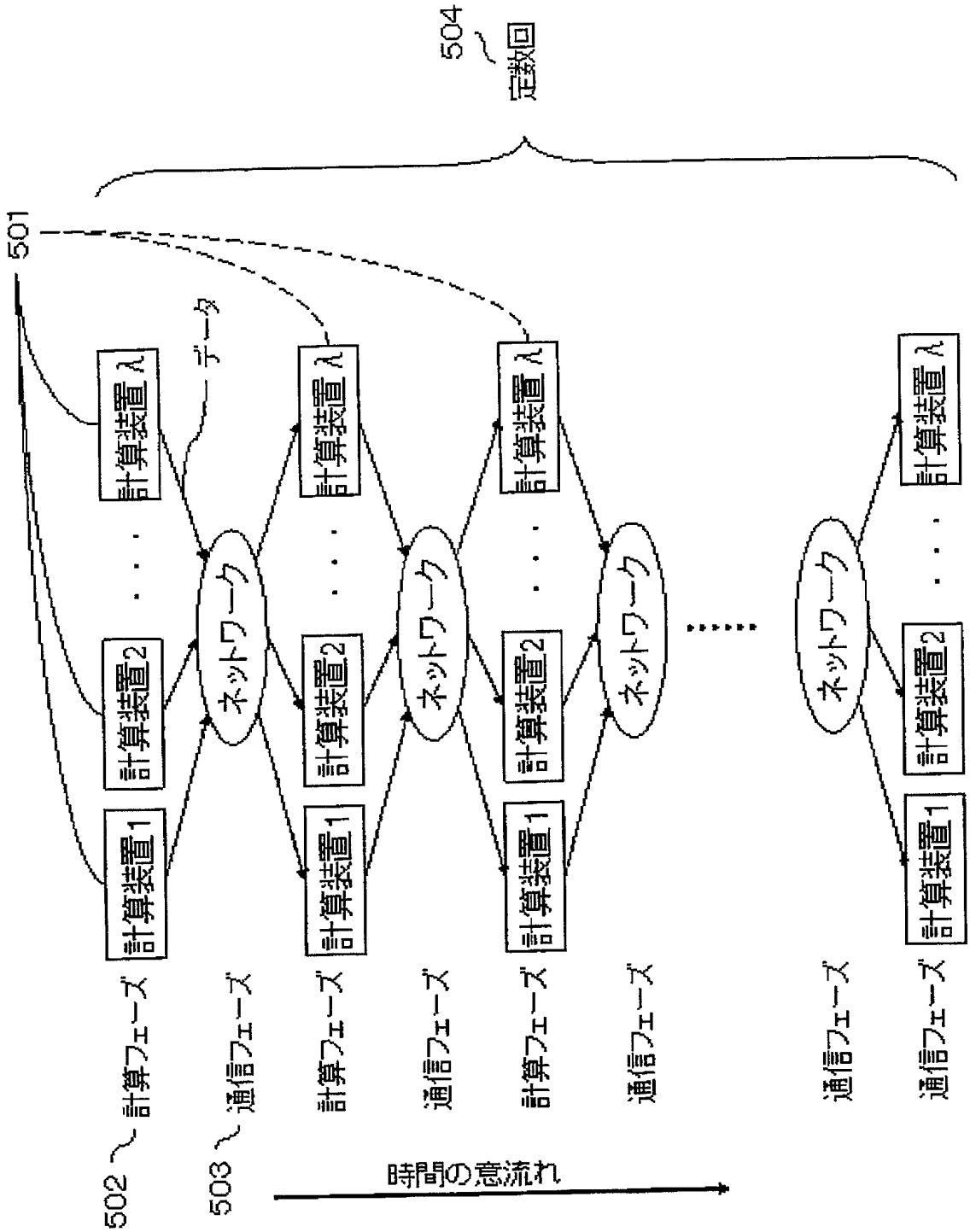
【図１２】第1の発明を実施するための最良の形態の構成を構成する計算装置の構成を示すブロック図である。

【図１３】第1の発明を実施するための最良の形態の動作の具体例における、入力処理の詳細を示すフローチャートである。
【図１４】第二の発明の装置の関係を示したブロック図。
【図１５】第二の発明で、各計算装置が一周目から三周目までの各周で行う計算のフローチャート
【図１６】第二の発明におけるデータの流れ。
【図１７】一周目の本計算のフローチャート
【図１８】二周目の本計算のフローチャート
【図１９】従来の技術における各ゲートに関して計算されるデータの理解を助けるための図である。

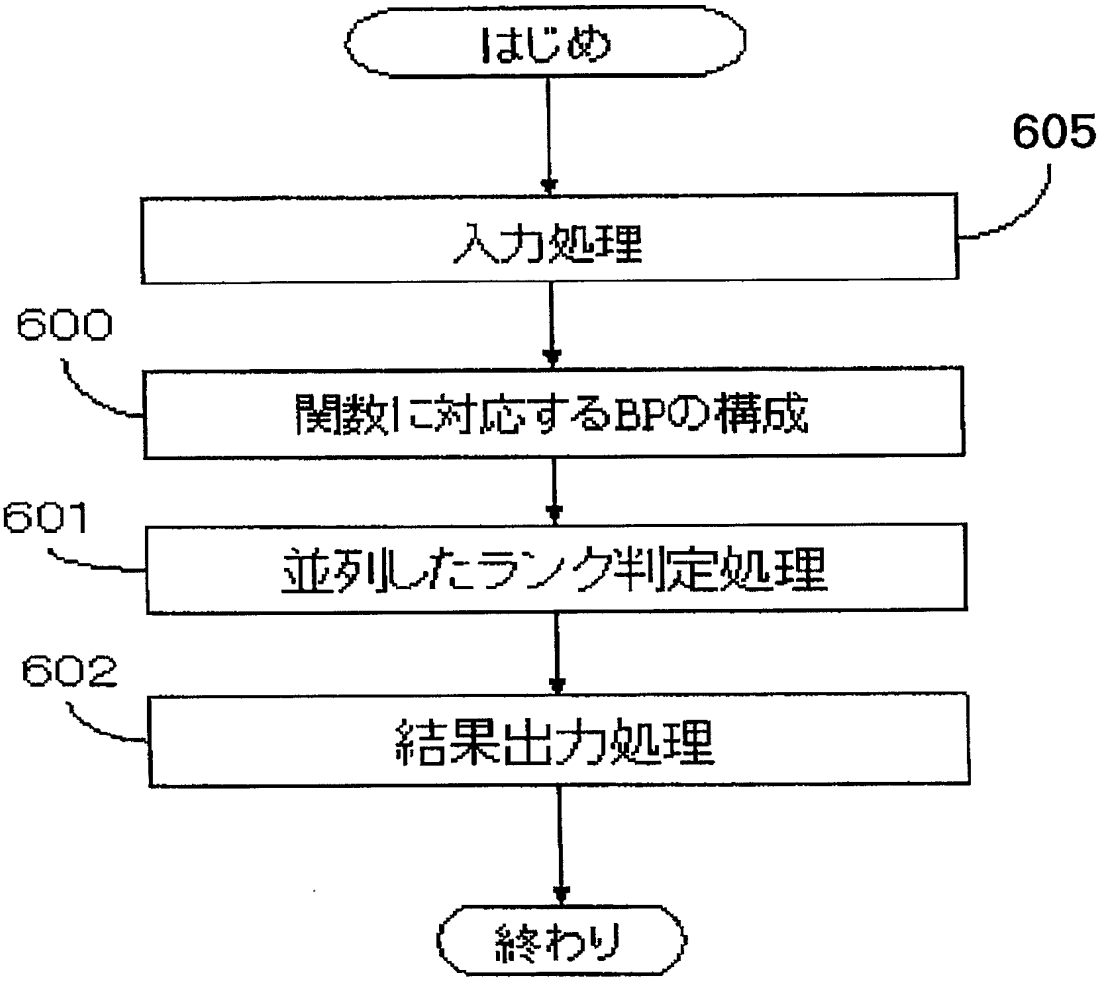
【書類名】図面
【図１】



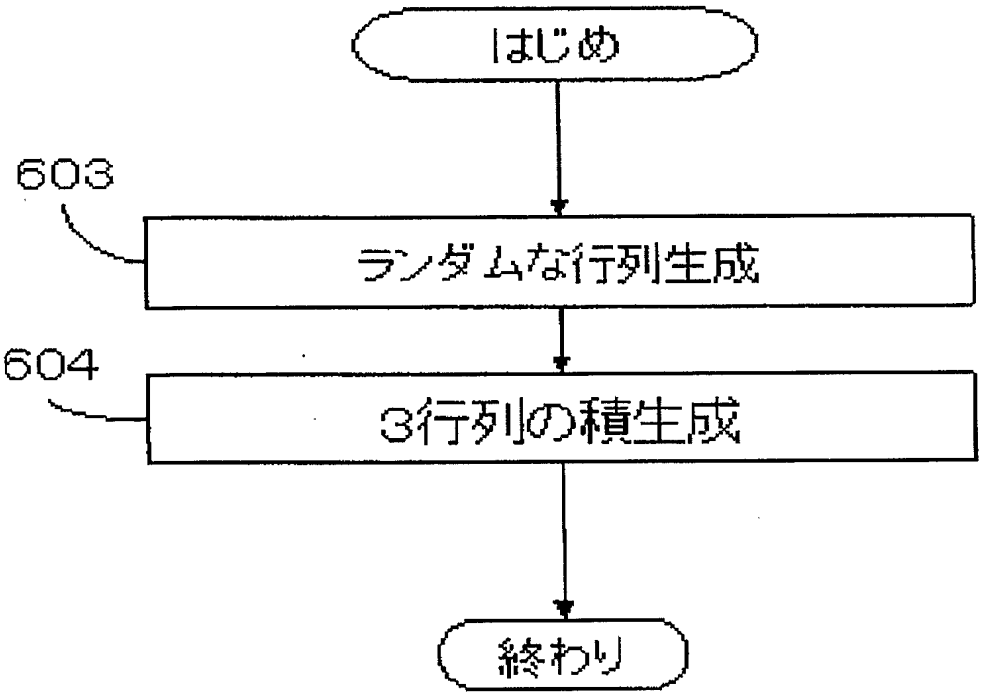
【図２】


504
定数回
501
データ
計算装置1
計算装置2
計算装置λ
ネットワーク
502 計算フェーズ
503 通信フェーズ
時間の意流れ

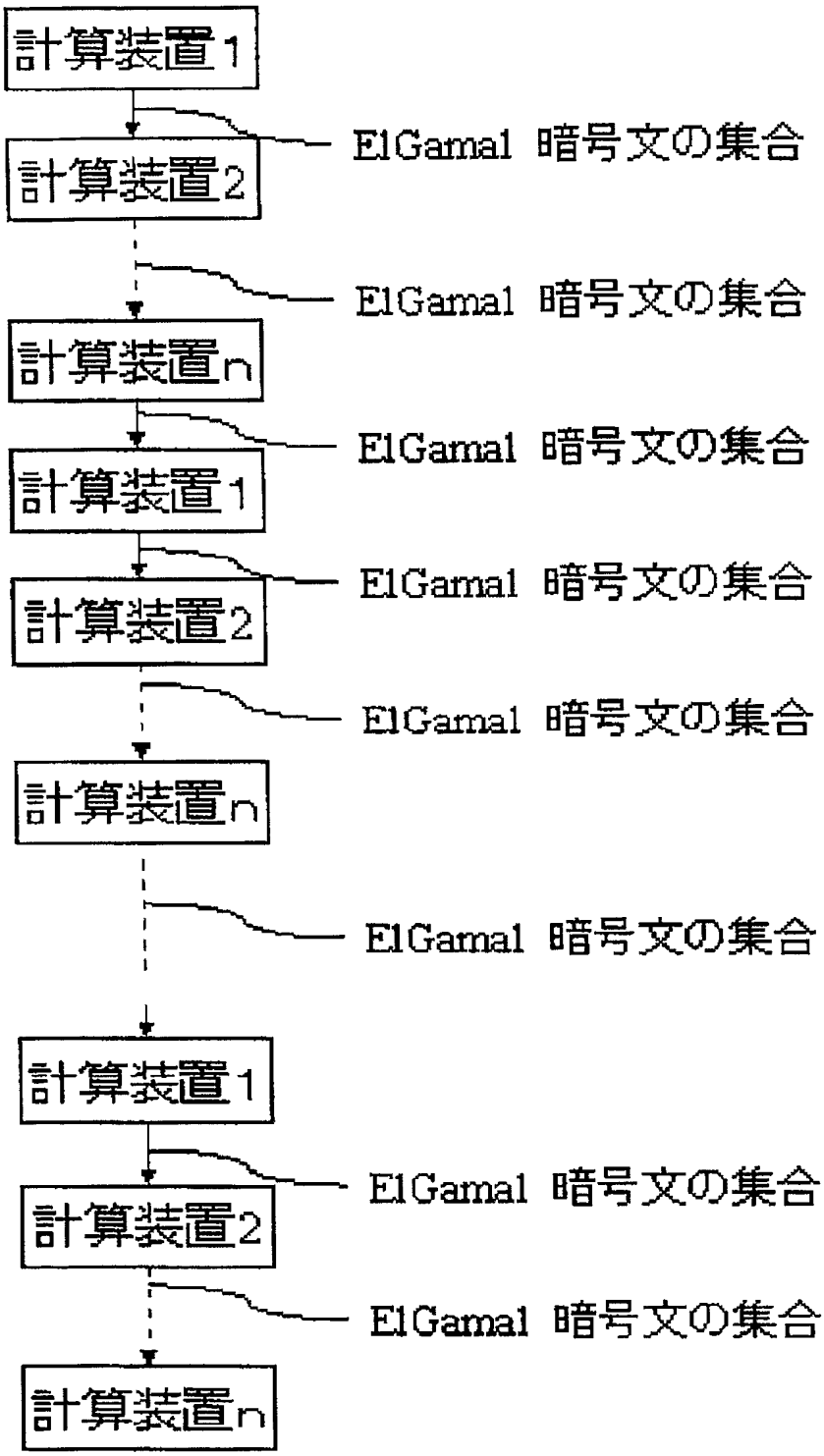
【図３】


はじめ
605
入力処理
600
関数Iに対応するBPの構成
601
並列したランク判定処理
602
結果出力処理
終わり

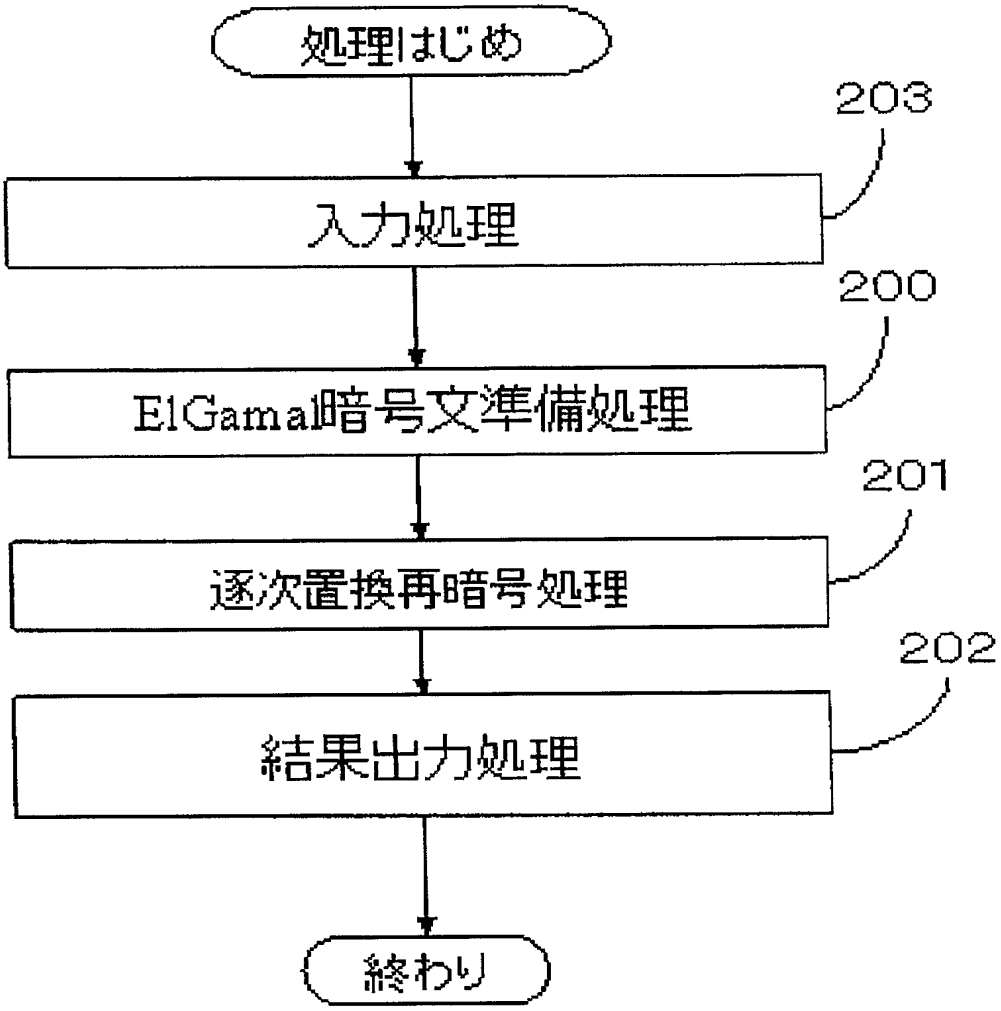
【図４】



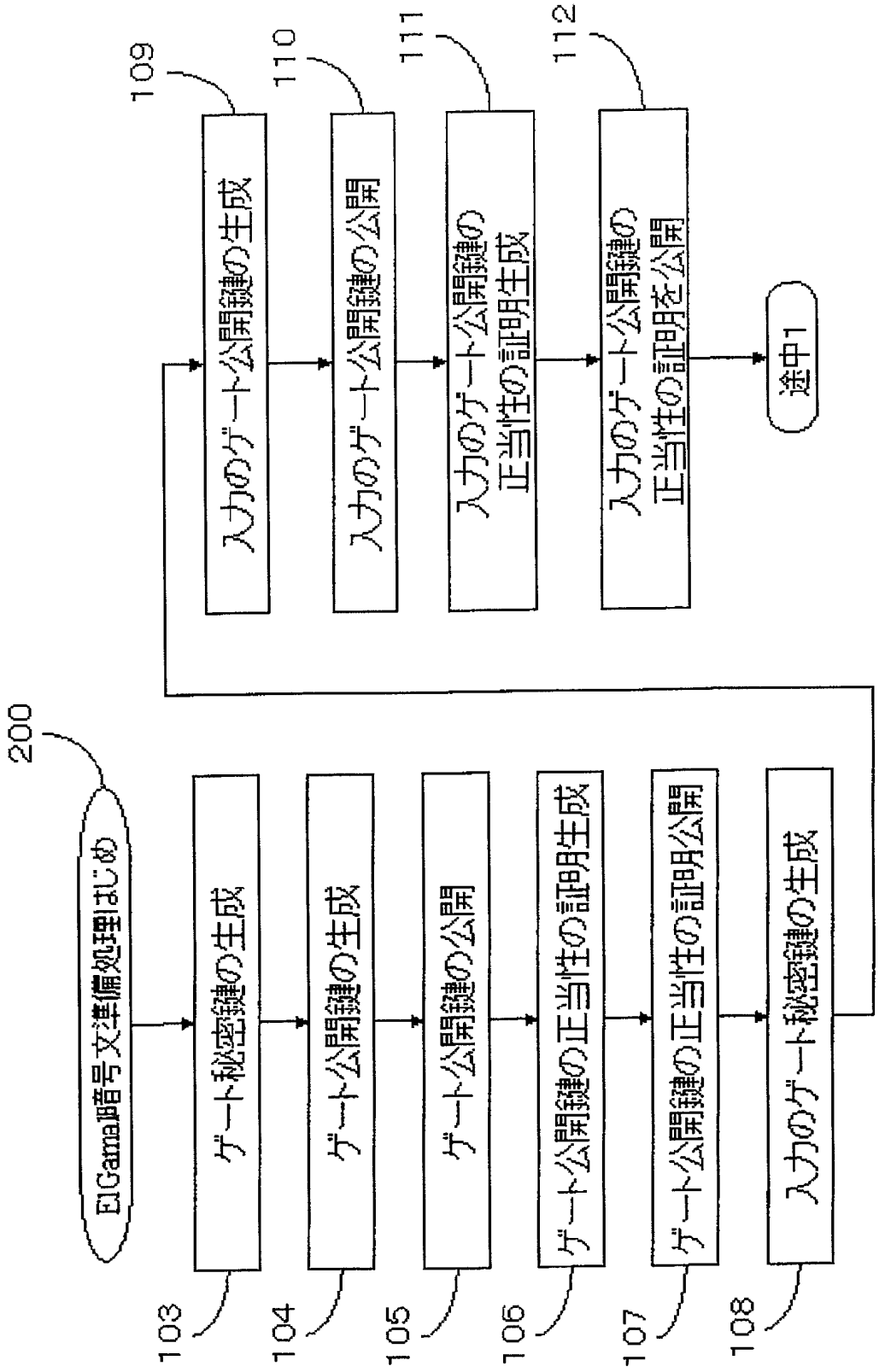
【図５】


計算装置1
ElGamal 暗号文の集合
計算装置2
ElGamal 暗号文の集合
計算装置n
ElGamal 暗号文の集合
計算装置1
ElGamal 暗号文の集合
計算装置2
ElGamal 暗号文の集合
計算装置n
ElGamal 暗号文の集合
計算装置1
ElGamal 暗号文の集合
計算装置2
ElGamal 暗号文の集合
計算装置n

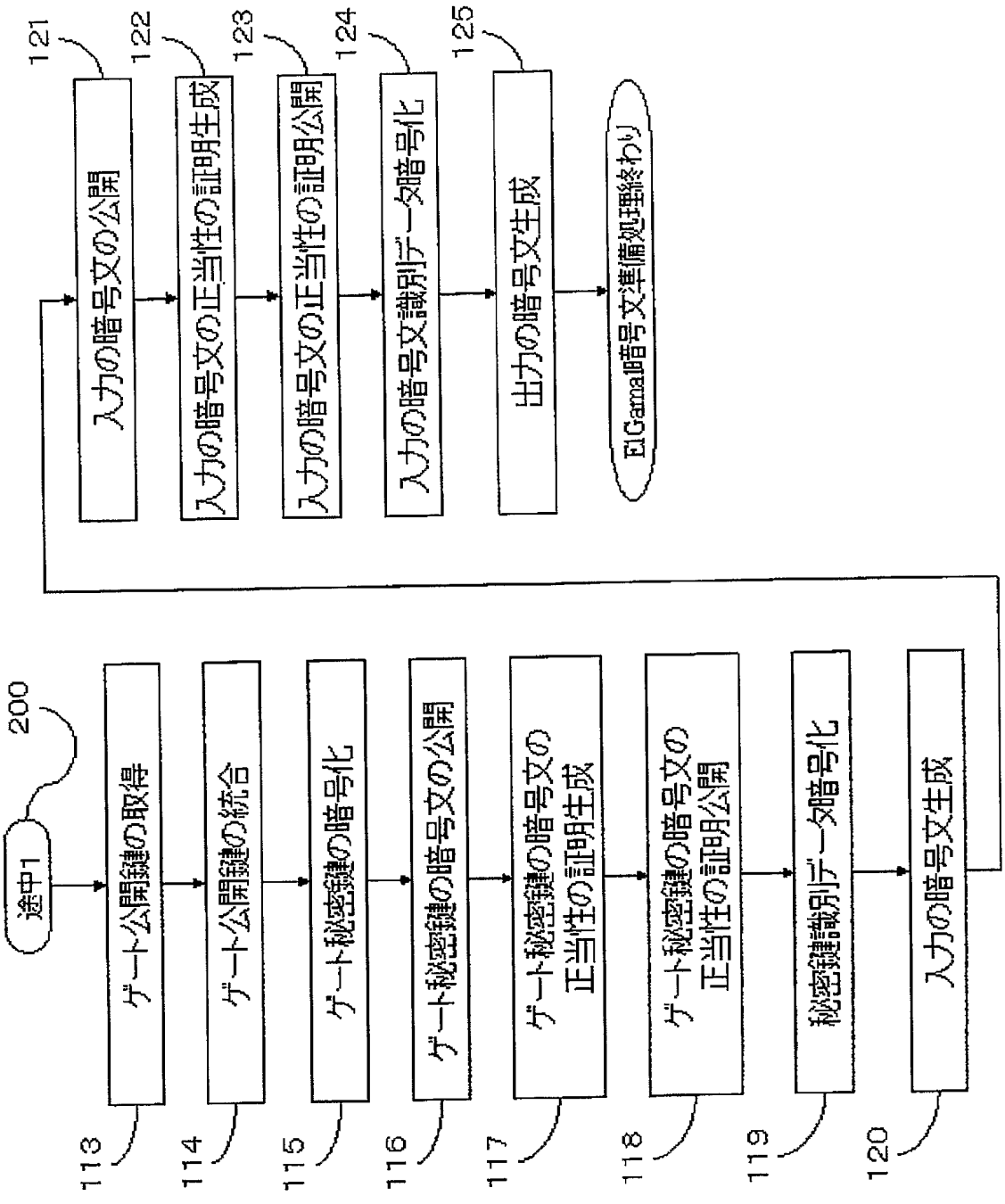
【図６】


処理はじめ
203
入力処理
200
ElGamal暗号文準備処理
201
逐次置換再暗号処理
202
結果出力処理
終わり

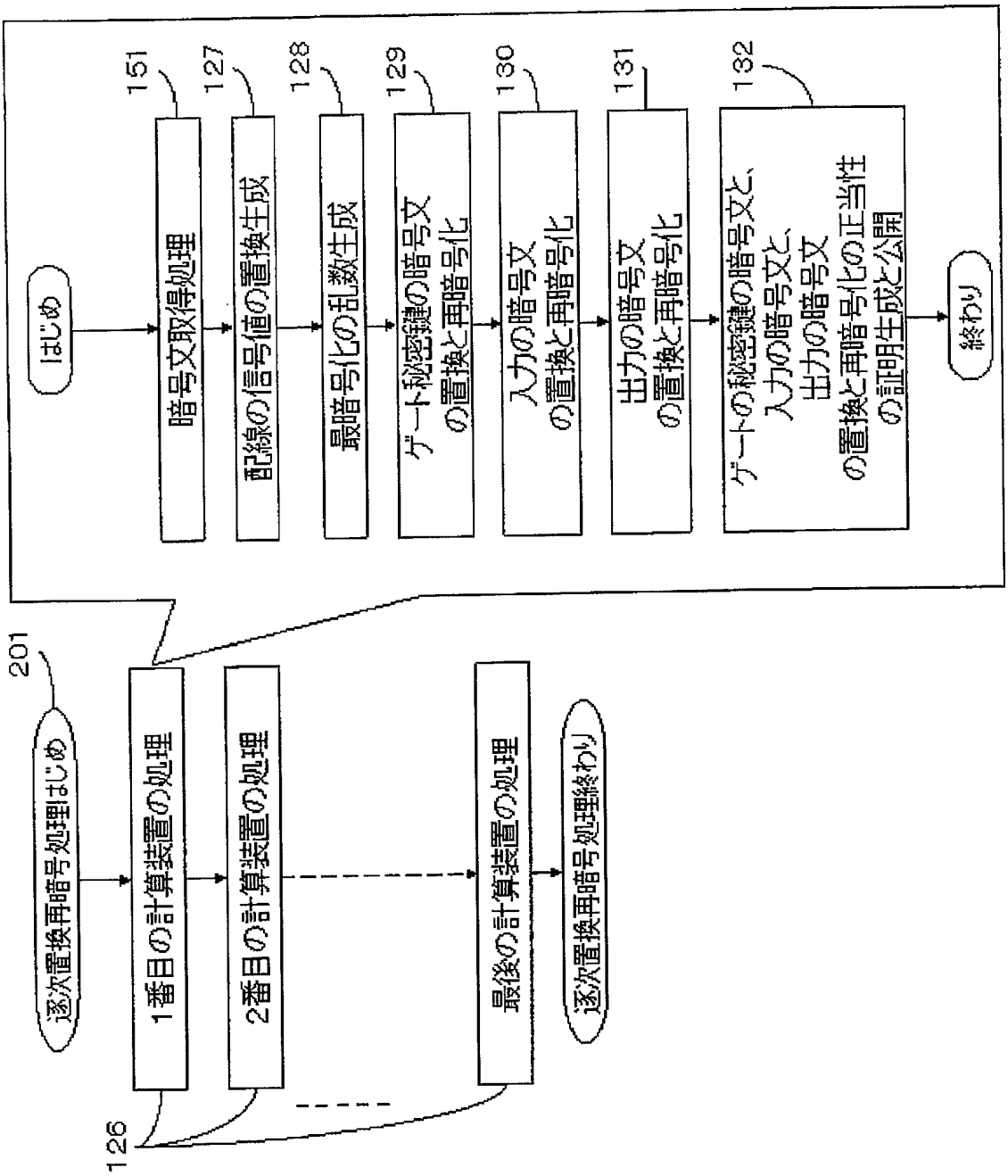
【図７】


200
ElGamal暗号文準備処理はじめ
103
ゲート秘密鍵の生成
104
ゲート公開鍵の生成
105
ゲート公開鍵の公開
106
ゲート公開鍵の正当性の証明生成
107
ゲート公開鍵の正当性の証明公開
108
入力のゲート秘密鍵の生成
109
入力のゲート公開鍵の生成
110
入力のゲート公開鍵の公開
111
入力のゲート公開鍵の
正当性の証明生成
112
入力のゲート公開鍵の
正当性の証明を公開
途中1

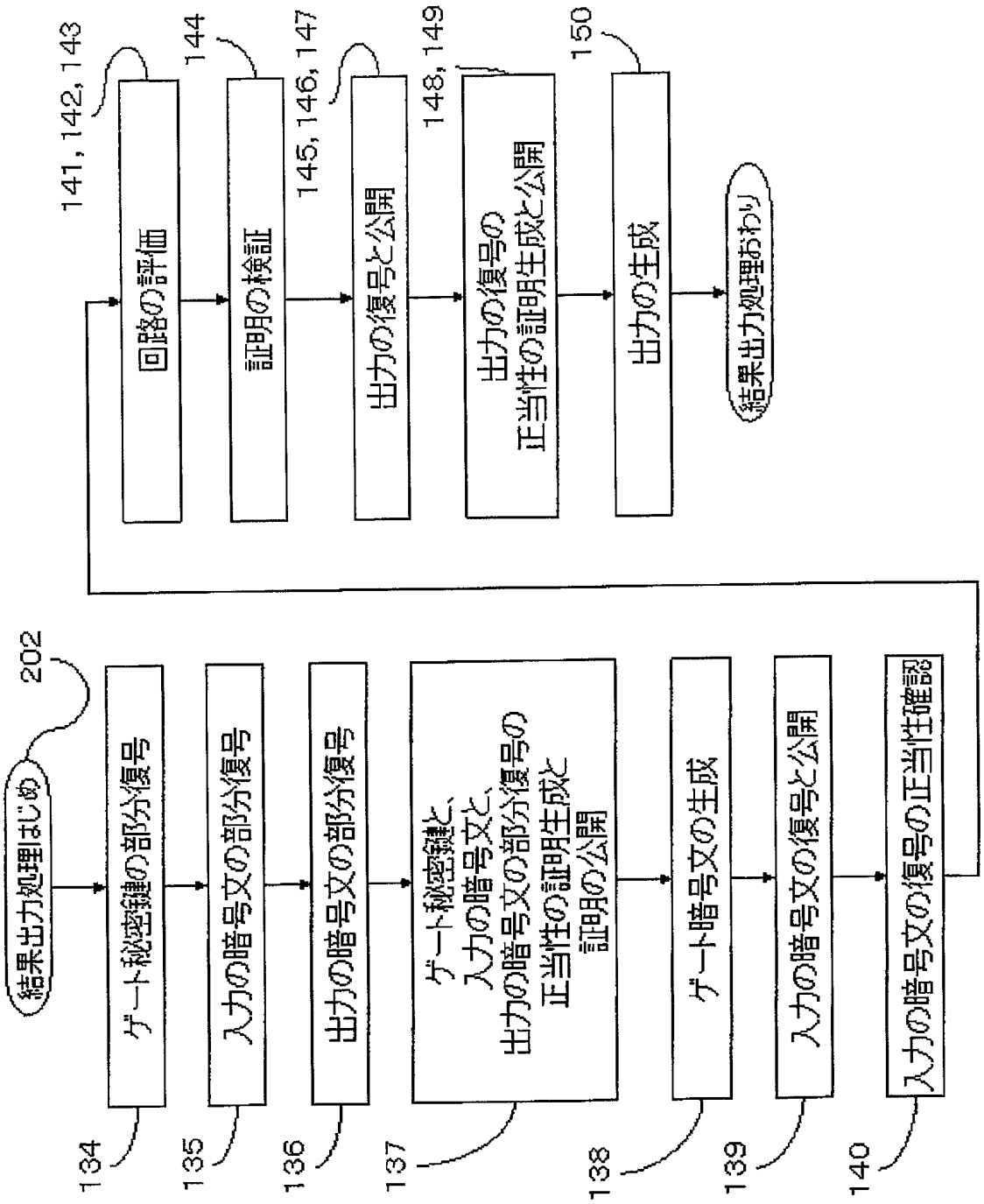
【図８】


途中1
200
ゲート公開鍵の取得
113
ゲート公開鍵の統合
114
ゲート秘密鍵の暗号化
115
ゲート秘密鍵の暗号文の公開
116
ゲート秘密鍵の暗号文の
正当性の証明生成
117
ゲート秘密鍵の暗号文の
正当性の証明公開
118
秘密鍵識別データ暗号化
119
入力の暗号文生成
120
入力の暗号文の公開
121
入力の暗号文の正当性の証明生成
122
入力の暗号文の正当性の証明公開
123
入力の暗号文識別データ暗号化
124
出力の暗号文生成
125
ElGamal暗号文準備処理終わり

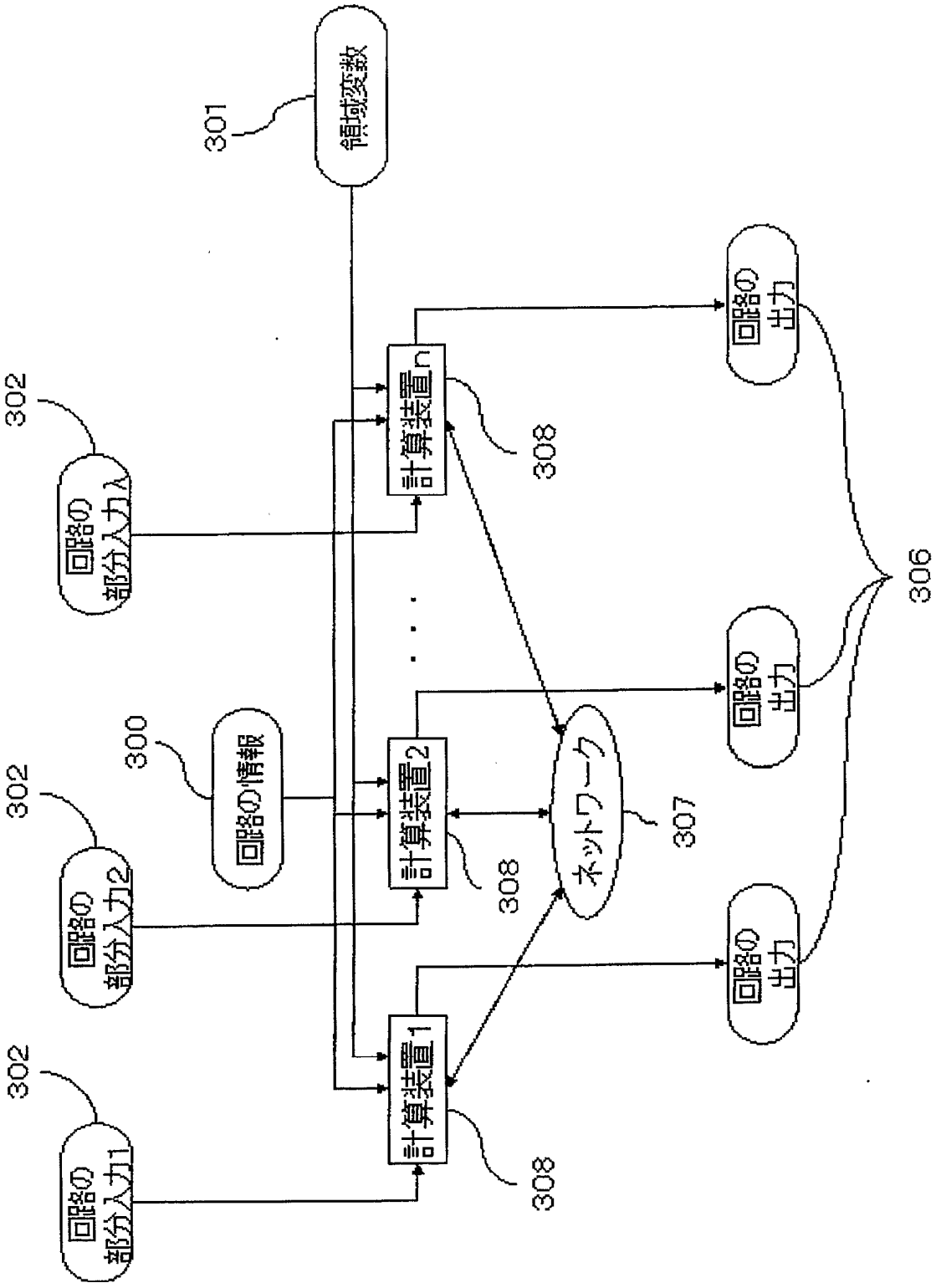
【図９】


はじめ
暗号文取得処理
151
配線の信号値の置換生成
127
最暗号化の乱数生成
128
ゲート秘密鍵の暗号文の置換と再暗号化
129
入力の暗号文の置換と再暗号化
130
出力の暗号文の置換と再暗号化
131
ゲートの秘密鍵の暗号文と、入力の暗号文と、出力の暗号文の置換と再暗号化の正当性の証明生成と公開
132
終わり
逐次置換再暗号処理はじめ
201
1番目の計算装置の処理
2番目の計算装置の処理
最後の計算装置の処理
逐次置換再暗号処理終わり
126

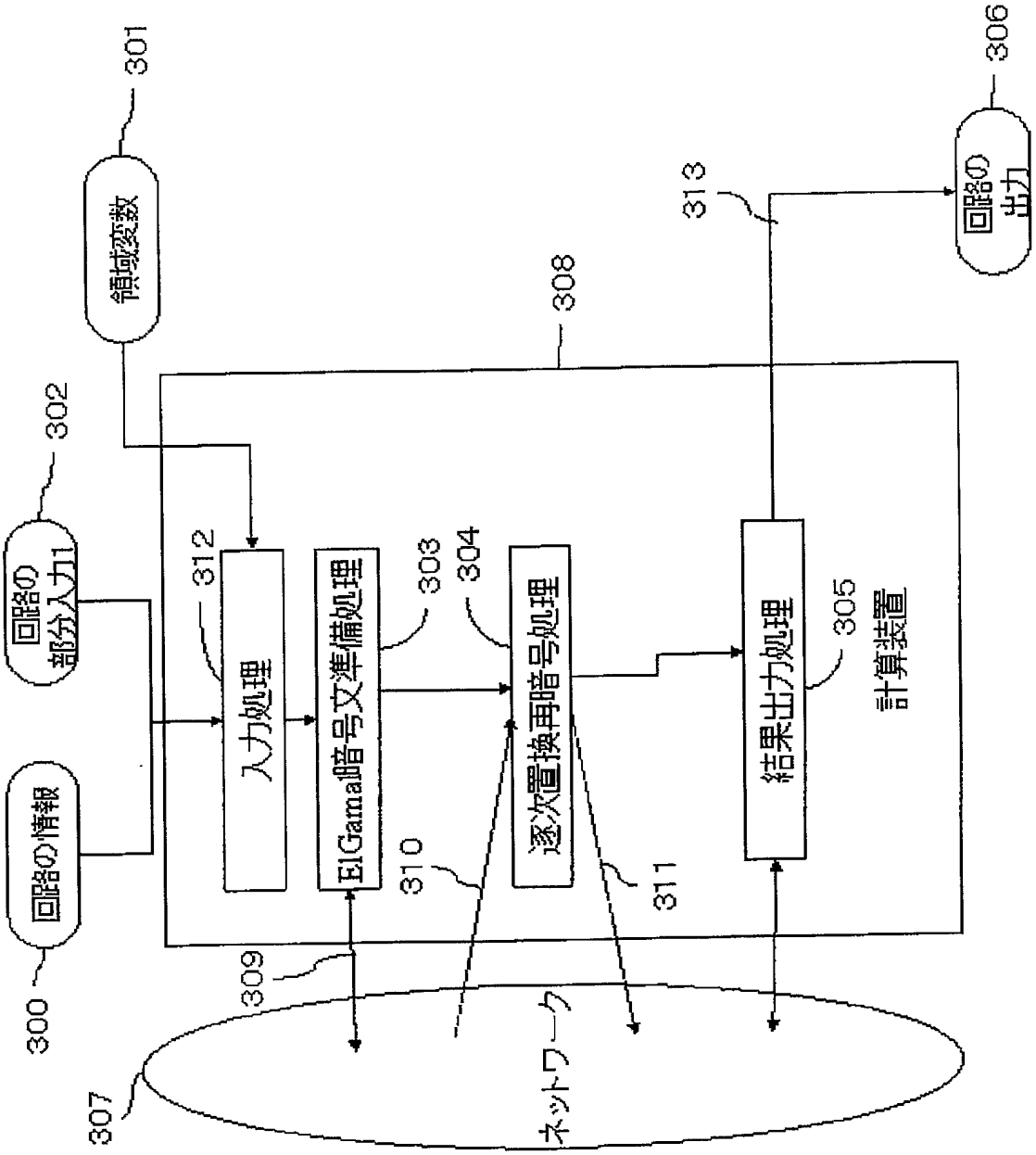
【図１０】


結果出力処理はじめ
202
ゲート秘密鍵の部分復号
134
入力の暗号文の部分復号
135
出力の暗号文の部分復号
136
ゲート秘密鍵と、
入力の暗号文と、
出力の暗号文の部分復号の
正当性の証明生成と
証明の公開
137
ゲート暗号文の生成
138
入力の暗号文の復号と公開
139
入力の暗号文の復号の正当性確認
140
回路の評価
141, 142, 143
証明の検証
144
出力の復号と公開
145, 146, 147
出力の復号の
正当性の証明生成と公開
148, 149
出力の生成
150
結果出力処理おわり

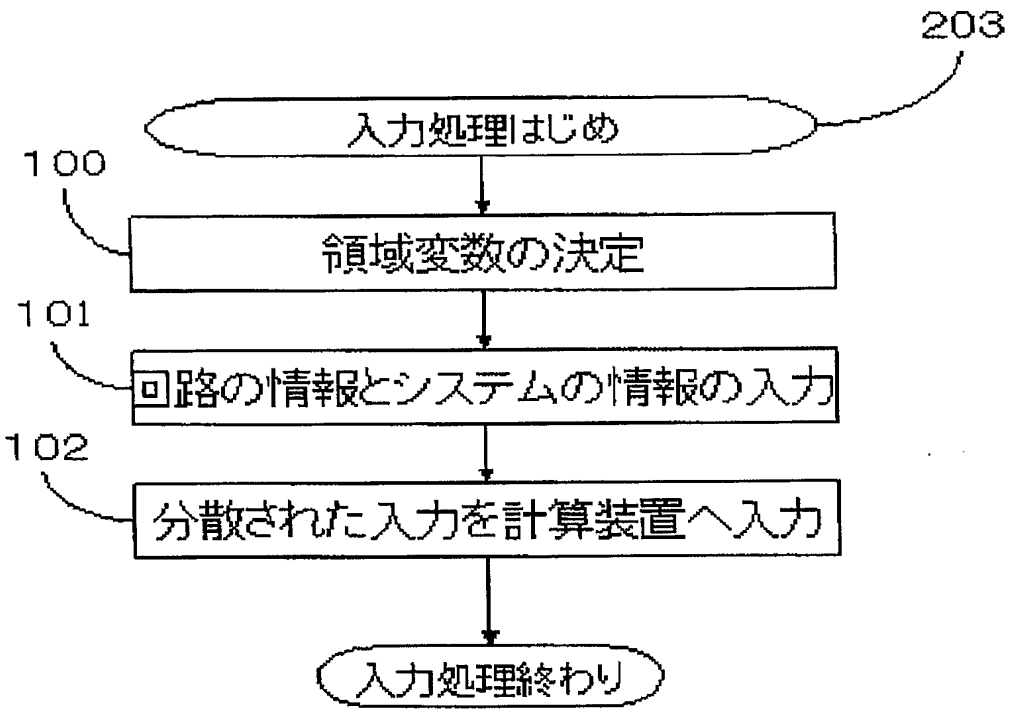
【図１１】


領域変数
301
回路の情報
300
回路の部分入力1
回路の部分入力2
回路の部分入力λ
302
計算装置1
計算装置2
計算装置n
308
ネットワーク
307
回路の出力
306

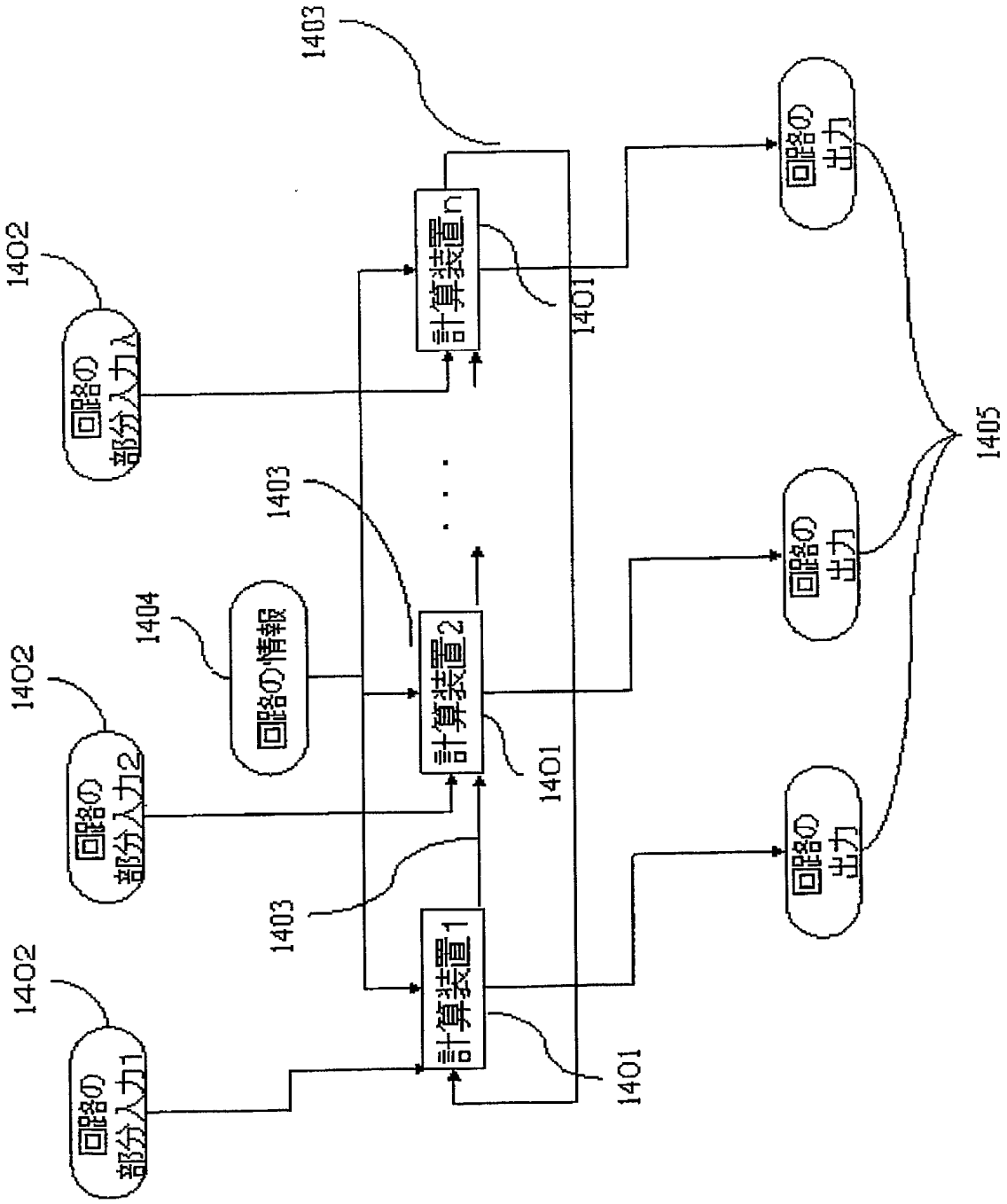
【図１２】


301
領域変数
306
回路の出力
313
308
302
回路の部分入力1
312
入力処理
303
ElGamal暗号文準備処理
304
逐次置換再暗号処理
305
結果出力処理
計算装置
回路の情報
310
311
309
300
307
ネットワーク

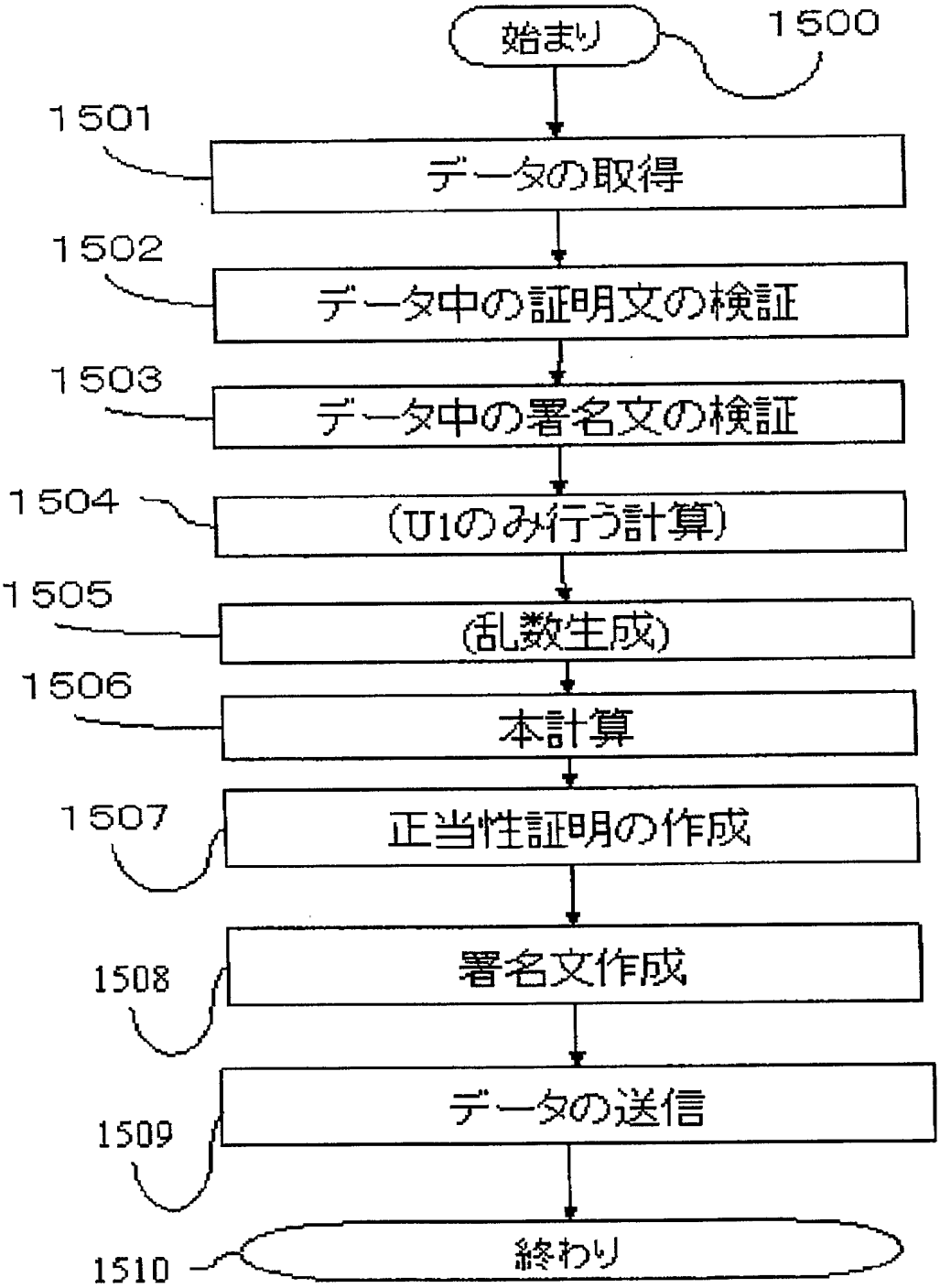
【図１３】


203
入力処理はじめ
100
領域変数の決定
101
回路の情報とシステムの情報の入力
102
分散された入力を計算装置へ入力
入力処理終わり

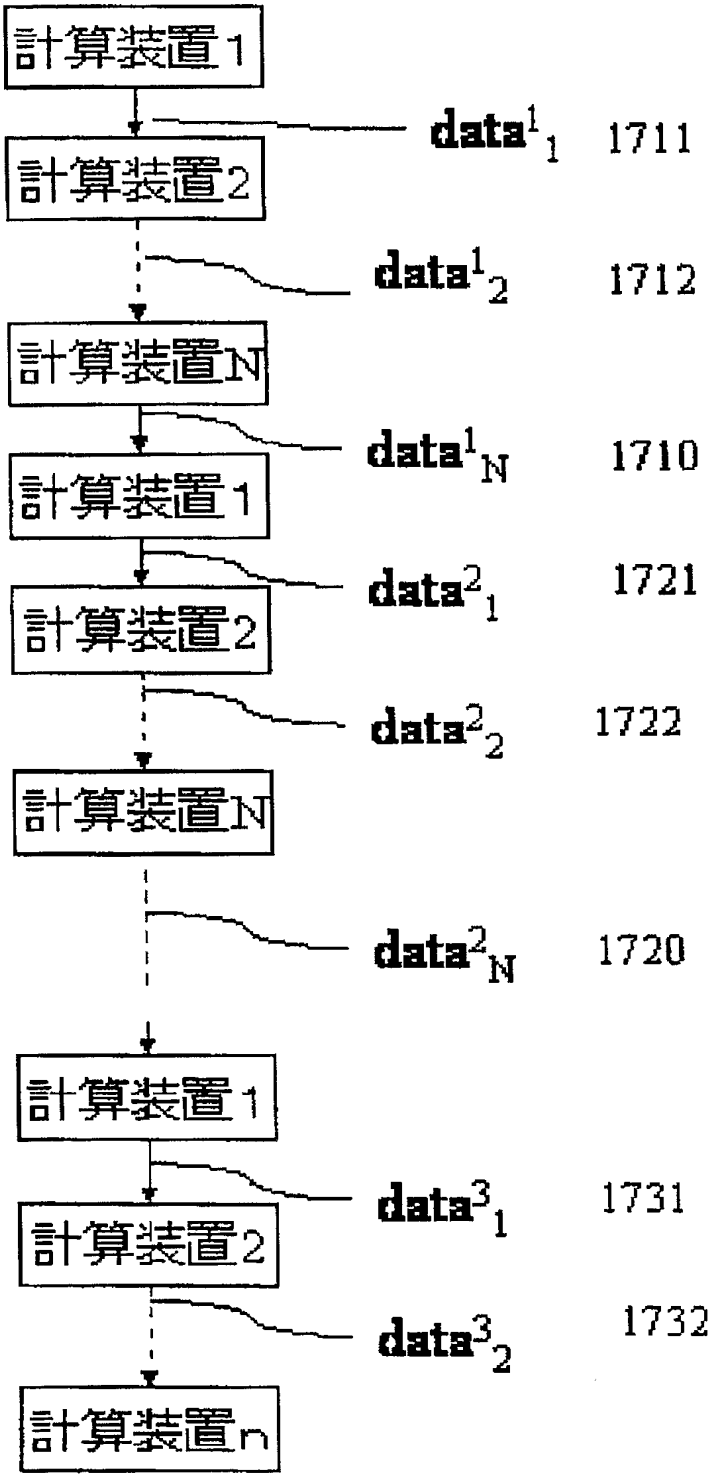
【図１４】


1403
1402
回路の部分入力n
計算装置n
1401
回路の出力
1405
1403
1404
回路の情報
1402
回路の部分入力2
計算装置2
1401
回路の出力
1403
1402
回路の部分入力1
計算装置1
1401
回路の出力

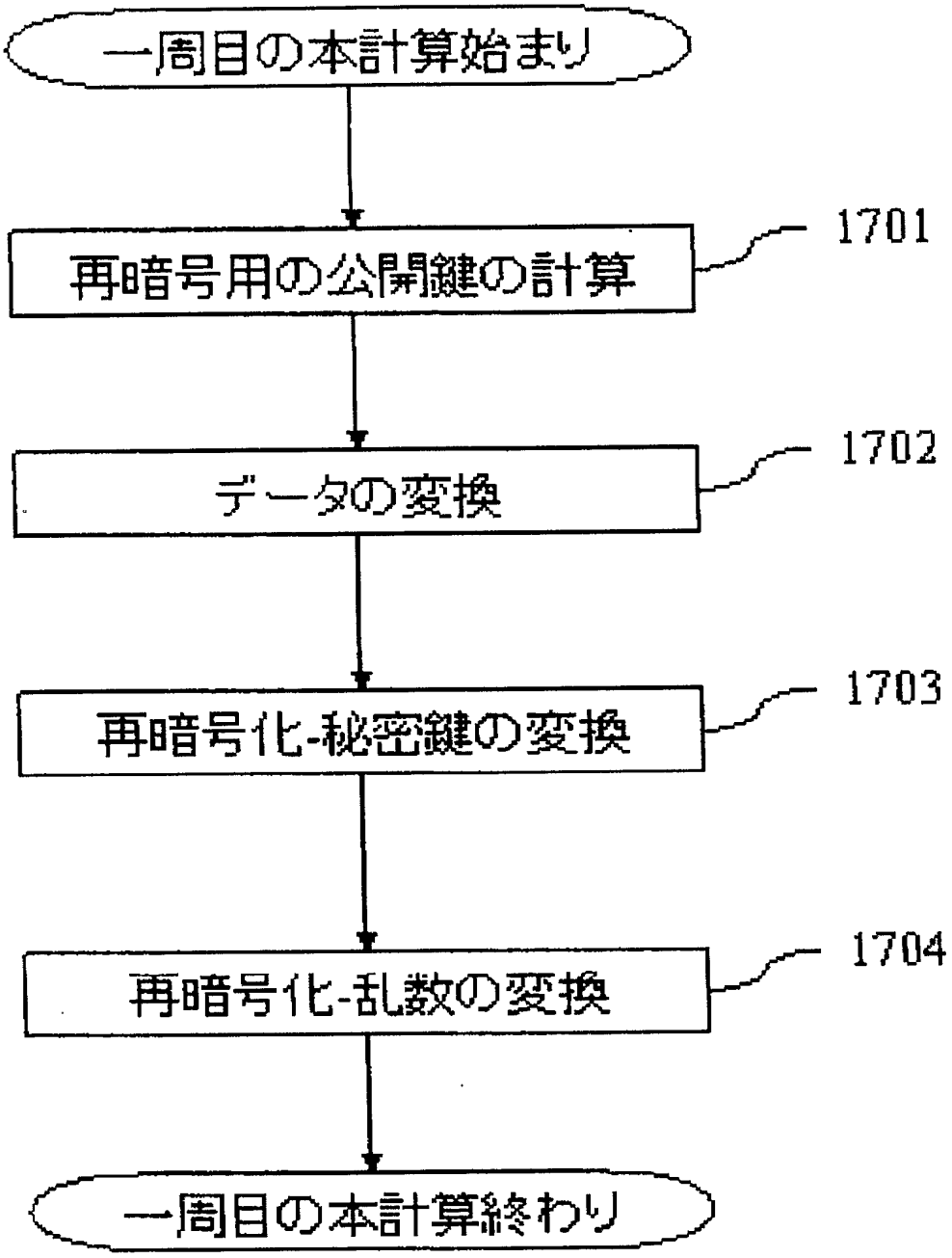
【図１５】


始まり
1500
1501
データの取得
1502
データ中の証明文の検証
1503
データ中の署名文の検証
1504
(U1のみ行う計算)
1505
(乱数生成)
1506
本計算
1507
正当性証明の作成
署名文作成
1508
データの送信
1509
終わり
1510

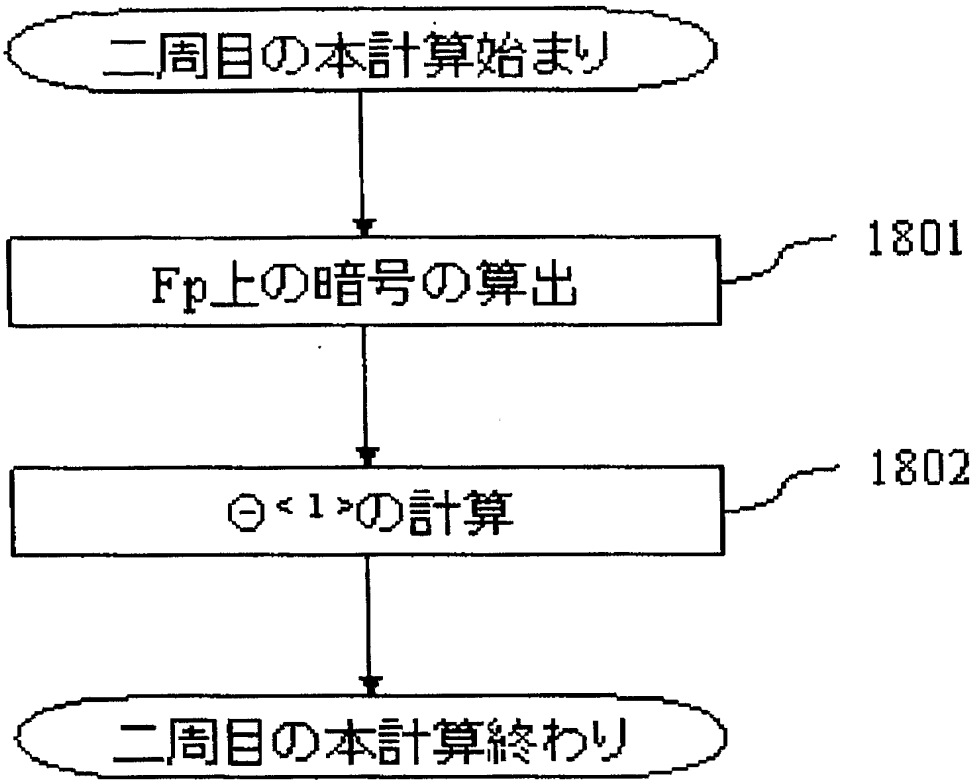
【図１６】


計算装置1
data$^1_1$ 1711
計算装置2
data$^1_2$ 1712
計算装置N
data^1_N 1710
計算装置1
data$^2_1$ 1721
計算装置2
data$^2_2$ 1722
計算装置N
data^2_N 1720
計算装置1
data$^3_1$ 1731
計算装置2
data$^3_2$ 1732
計算装置n

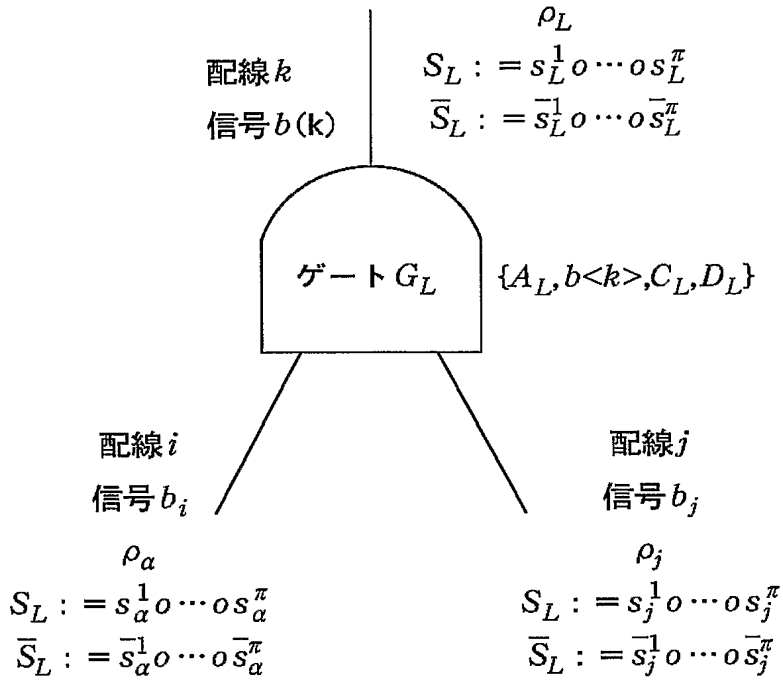
【図１７】


一周目の本計算始まり
再暗号用の公開鍵の計算
1701
データの変換
1702
再暗号化-秘密鍵の変換
1703
再暗号化-乱数の変換
1704
一周目の本計算終わり

【図１８】



【図１９】


ρ_L
$S_L := s_L^1 o \cdots o s_L^\pi$
$\overline{S}_L := \overline{s}_L^1 o \cdots o \overline{s}_L^\pi$
配線k
信号b(k)
ゲートG_L
$\{A_L, b<k>, C_L, D_L\}$
配線i
信号b_i
配線j
信号b_j
ρ_α
$S_L := s_\alpha^1 o \cdots o s_\alpha^\pi$
$\overline{S}_L := \overline{s}_\alpha^1 o \cdots o \overline{s}_\alpha^\pi$
ρ_j
$S_L := s_j^1 o \cdots o s_j^\pi$
$\overline{S}_L := \overline{s}_j^1 o \cdots o \overline{s}_j^\pi$

【書類名】要約書
【要約】
【課題】　複数の計算装置を含む機器を用いて与えられた関数の値を計算することをより簡単な構成で実現する。
【解決手段】入力処理では、複数の計算装置に、回路と、回路への入力ビットとが入力され、まず一台の計算装置が計算を行い、その計算結果を他の計算装置のうち一台に送り、次にその計算結果を受け取った前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする。
【選択図】　図６

特願２００４－０１６８８１

出　願　人　履　歴　情　報

識別番号　［０００００４２３７］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社